MORETELE LOCAL MUNICIPALITY

ICT CHANGE CONTROL MANAGEMENT POLICY

Policy number	ICT-007-2026
Date of Management engagement	26 June 2026
Resolution Number	13001001-06-2026
Council Approval	30 June 2026
Review Date	26 June 2027
Signature: Municipal Manager	

Change Record

Author	Date	Version	Change
Moretele Local Municipality	April 2023	1	

Reviewers

Name	Date	Version
ICT Unit	April 2023	2
ICT Steering committee	April 2023	2

Name	Date	Version
ICT Unit	23 June 2026	3
ICT Steering committee	26 June 2026	3

Table of Contents

1. SCOPE

The Change Control policy is established to

- Provide guidance and oversight of the configuration and change control processes for systems included in the municipalities' projects. These systems include Management Information and any other Computer-related Systems.
- Sets strategic direction and priorities for Information Management.
- Reviews and approves recommendations for Information Management
- Standards, policies and procedures, and reviews issues of non-compliance
- Ensures senior management and other stakeholders have input into the planning process.
- Reviews and endorses recommendations for allocation and commitment of resources, annual Information Systems capital budgets and large projects to appropriate decision-making authorities.
- Provides ongoing oversight review of large projects and initiatives at pre-defined Milestones.

2. PURPOSE

The purpose of the Change Control Policy is:

- To review, approve/not approve, prioritize, and manage production system customizations or modifications in an organized and timely manner. The goal is to limit production software changes and effectively manage the impact of those changes on project schedules, costs, and existing and planned information systems.
- Aligns information management strategies with overall organizational mission
- Facilitates the achievement of optimal information management.
- Encourages constituent ownership of IT initiatives and endorsement of ICT policies.
- Encourages a collaborative work environment and fosters trust via mutual credibility and responsiveness.

3. OBJECTIVE

The objective of this Change Control Management Policy is to ensure that all changes to information systems, applications, infrastructure, and related processes are identified, evaluated, approved, implemented, and reviewed in a controlled and consistent manner.

This policy aims to:

- Minimize disruptions to services and operations
- Reduce risks associated with unauthorized or poorly managed changes
- Maintain system integrity, security, and compliance
- Ensure proper documentation, accountability, and traceability of all changes
- Improve overall service quality and operational efficiency

4. CHANGE CONTROL PROCESS

Change Control is the overall process for management of the preparation, justification, evaluation, coordination, and implementation of proposed changes to the Systems of Municipality. Change Control begins after software products are migrated into the production environment. The following process shall be utilised for submitting proposed system changes and determining approval/disapproval of those changes:

4.1 APPLICABILITY OF THE POLICY

4.1.1 This policy applies to all employees of the Municipality, including Contractors and Consultants, who use ICT services and assets.

4.1.2 This policy is supported by a range of security controls documented within operating Policies, technical controls embedded in information systems and other controls that will be advised to employees.

5. PRINCIPLES

The purpose of this policy is to establish management direction and high-level objectives for change management. This policy will ensure the implementation of change management strategies to mitigate associated risks such as:

a. Information being corrupted or destroyed.
b. Computer performance being disrupted or degraded.

c. Productivity losses being incurred.
d. Exposure to reputational risk

6. APPLICATION

6.1 Policy

a. The change management process shall be formally defined and documented, to control changes to all critical information resources (such as hardware, software, system documentation and operating Policies). This process shall include management responsibilities and Policies. Wherever practical, operational and application change management Policies should be integrated.
b. At a minimum the change management process should include the following phases:

i. Logged Change Requests
ii. Identification, prioritisation and initiation of change
iii. Proper authorisation of change
iv. Requirements analysis
v. Inter-dependency and compliance analysis
vi. Impact Assessment
vii. Change approach
viii. Change testing
ix. User acceptance testing and approval
x. Implementation and release planning
xi. Documentation
xii. Change monitoring
xiii. Defined responsibilities and authorities of all users and ICT personnel
xiv. Emergency change classification parameters

6.2 Documented Change

Person or office initiating the proposed change will submit the Change request form (CRF). The business need must be identified on the Change request form.

The CFO must review the Change request form and obtain any necessary input from technical or functional staff. If the Departmental head concurs

with the need for the change, he/she will sign and forward the Change request form with any supporting documentation to ICT for implementation. The ICT Division shall maintain a documented audit trail, always containing relevant information. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

The ICT Unit and System Vendor will need to assign a priority designation to the Change request form selecting high, medium, or low.

- **High** priority modifications are items that are critical to production, processing, and must be completed as soon as possible. They are often statutory mandated and based on a change in regulation or statute or required to correct a software failure or system halt in the production environment.

- **Medium** priority modifications are items that may be highly visible to external entities or may affect the technical integrity of the software but does not halt production.

- **Low** priority modifications are neither production critical or highly visible. Generally, these changes are considered system enhancements or may be specific to a local organization.

7) Changes are made on UAT server first for testing purposes.

Before any changes are made on live system a backup should be made first.

When test is successful, change is migrated to live system, and change request form is signed off by System Administrator, CFO and Expenditure/Revenue Manager.

6.3 Risk Management

- A risk assessment shall be performed for all changes and depending on the outcome, an impact assessment should be performed.
- The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact

assessment should, where applicable consider compliance with legislative requirements and standards.

6.4 Change Classification

- All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.

6.5 Testing

- Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

6.6 Changes Affecting Service Level Agreements

- The impact of change on existing Service Level Agreements (SLA) shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

6.7 Version Control

- Any software change or update shall be controlled with version control. Older versions shall be archived.

6.8 Approval

- All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

6.9 Communicating Changes

- All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change request form. Users shall be required to make submissions and comment prior to the acceptance of the change.

6.10 Implementation

- Implementation will only be undertaken after appropriate testing and approval by Change Committee. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

6.11 Roll Back

- Policies for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), Policy's and responsibilities shall be noted for the recovery and continuity of the affected areas.
- Fall back Policy's shall be in place to ensure systems can revert to what they were prior to implementation of changes.

6.12 Documentation

- Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.
- Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and Policy's, affected by software changes, shall be updated on completion of each change.

6.13 Disaster Recovery Plan (DRP)

- The Disaster Recovery Plan shall be updated with relevant changes, managed through the change control process. The Disaster Recovery Plan and continuity plans rely on the completeness, accuracy and availability of DRP documentation.
- DRP documentation is the road map used for minimal disruption in business continuity.

6.14 Emergency Changes

- Specific Policy's to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.
- Classification Criteria:

  Critical Service Disruption

  Immediate action is required to restore or prevent the failure of a critical system or service.

  Information Security Incident
  Urgent changes are needed to remediate security vulnerabilities, breaches, or cyber threats.

  Regulatory or Legal Requirement
  Immediate compliance is required to meet legislative, regulatory, or audit obligations.

  Risk to Data Integrity or Availability
  The change is necessary to prevent or resolve data loss, corruption, or unavailability.

  Health, Safety, or Environmental Risk
  The change is required to mitigate risks that could impact the safety of individuals or the environment.

  Significant Business Impact
  Any issue that, if not addressed immediately, would result in substantial financial loss, reputational damage, or operational failure.

- Authorisation Requirements:
  Emergency changes may be implemented with expedited approval from designated authorities (e.g. Head of department, or delegated authority).

- Documentation and Audit Trail:
  All emergency changes must be fully documented in the change management system as soon as practicable.

6.15 Change Monitoring

- All changes shall be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

7. ROLES AND RESPONSIBILITIES

7.1 The Change Committee shall:

The Change Advisory Board (CAB), shall be established to provide governance, oversight, and decision-making authority over all significant changes affecting ICT systems and services.

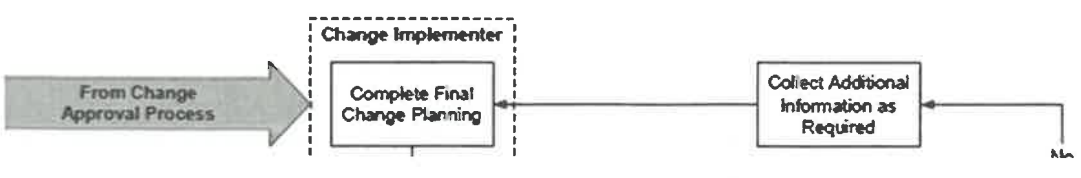
The CAB ensures that all changes are:

- Properly assessed for risk, impact, and business value
- Aligned with organizational priorities and compliance requirements
- Approved in a controlled and consistent manner
- Scheduled and coordinated to minimize disruption

7.2 The ICT Manager shall:

a. Ensure that all users are aware of the applicable policies, standards, Policy's and guidelines for change management.
b. Ensure that policy, standards and procedural changes are communicated to applicable users and management.
c. Evaluate change request and potential risks and introduce counter measures to address these risks.
d. Facilitate and coordinate the necessary change management Policys within the Municipality.
e. Report and evaluate changes to change management policies and standards.
f. Coordinate the implementation of new or additional security controls for change management.
g. Review the effectiveness of change management strategy and implement remedial controls where deficits are identified.
h. Coordinate awareness strategies and rollouts to effectively communicate change management mitigation solutions.

8. CHANGE MANAGEMENT WORKFLOW



9. POLICY REVIEW

This policy shall be reviewed on an annual basis by the ICT steering committee members to:

- Determine if there have been changes in International, National or Internal references that may impact on this policy.
- Determine if there are improvements or changes in the ICT process that should be reflected in this policy.

10. TERMS AND DEFINITIONS

TERM	DEFINITION
Incident	Any event which is not part of the standard operation of a service which causes, or may cause, an interruption to, or a reduction in, the quality of that service.
Standard	Guideline documentation reflects agreements on products, practices, or operations by nationally or internationally recognized industrial, professional, trade associations or governmental bodies.
System	An integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective (ISO12207, 1995:5)
User	An individual utilising Information Systems to achieve the business goals required to realise the mandate.

11. ACRONYMS

COBIT	Control Objectives for Information Technology
ICT	Information and Communication Technology
ICTSC	Information and Communication Technology Steering Committee
ITIL	Information Technology Infrastructure Library

12. REFERENCES

12.1 International Guidelines

- Control Objectives for Information Technology (COBIT)

12.2 International Standards

- Information Technology Infrastructure Library (ITIL)
- ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management

12.3 National Policy

- Constitution of the Republic of South Africa, Act 108 of 1996

- The Electronic Communications and Transactions (ECT) Act 25 of 2002
- National Strategic Intelligence Act 2 of 2000 applicable for South Africa
- Regulation of Interception of Communications Act 70 or 2002
- State Information Technology Act 88 of 1998.

---------- End of Document ----------