MANDENI MUNICIPALITY

ICT CHANGE CONTROL POLICY 2026-2027

Document No.	Revision	Print Date	Page
	0.1		Page 1 of 13

Table of Contents

LIST OF TABLES

APPROVAL AND REVISION HISTORY

APPROVAL SIGNATURES RECORD			
APPROVALS	CHAIRPERSON NAME	SIGNATURE	DATE

REVISION NUMBER	PAGE NUMBER/S	CHANGES EFFECTED	DATE OF CHANGE
0.1	1-10	First draft created	24-10-2022
0.2	1-12	Second draft created (review)	23-07-2026

GLOSSARY OF TERMS AND ABBREVIATIONS

Table 1: Terms and Abbreviations

Term/Abbreviation	Definition
Change Advisory Committee	Change Advisory Committee is a specific committee within the Municipality. It can be technical staff and crucial decision-makers such as member of the change management team, representative from all groups impacted by the change and ICT management. They are tasked with assessing changes to the ICT setting and authorising ICT services change during the change management process. In the context of Mandeni Local Municipality the ICT Steering Committee plays role for such Committee.
Directive	Refers to an instruction that come from a higher level of authority to the employees.
ICT	Refers to Information and Communication Technology
ICT Infrastructure	Refers to the information and communications technology infrastructure and systems (including software, hardware, firmware, networks and the Municipal Websites) that are used in the Municipality.
Information resources	All data and information as well as hardware and software.
MLM	Mandeni Local Municipality
Personnel	Includes employees/staff/officials employed permanently and temporarily by the Municipality.
Roll back	To uninstall or remove a change and restore a system to its previous state.
SIP	Refers to Service Improvement plan

1. SCOPE

This Change Control Policy applies to all changes made to the Municipality's ICT infrastructure, systems, applications, networks, databases, information resources, security controls, configurations, and technology services that may affect the availability, confidentiality, integrity, performance, or security of municipal ICT services.

The policy applies to:

- All planned, standard, normal, emergency, and urgent changes to municipal ICT environments.
- Changes to hardware, software, applications, operating systems, databases, networks, telecommunications, cloud services, security solutions, and ICT infrastructure.
- Changes to ICT configurations, security settings, access configurations, system parameters, and technical controls.
- Changes to production, development, testing, and disaster recovery environments.
- Changes implemented by Municipality employees, ICT personnel, contractors, consultants, service providers, and third parties.
- Changes resulting from new systems, system upgrades, maintenance, patches, configuration changes, technology replacements, cybersecurity requirements, legislative requirements, and business requirements.
- Emergency changes required to address critical incidents, cybersecurity threats, system failures, vulnerabilities, or other circumstances requiring immediate action.
- The complete change lifecycle, including change initiation, recording, categorisation, impact and risk assessment, approval, planning, testing, implementation, documentation, validation, and post-implementation review.
- Changes that may have an impact on business continuity, information security, data protection, cybersecurity, service availability, or regulatory compliance.

All changes shall be appropriately documented, assessed, authorised, tested where applicable, implemented in a controlled manner, and monitored.

No unauthorised change shall be introduced into the Municipality's ICT environment. Emergency changes shall follow an expedited approval and documentation process and shall be retrospectively reviewed.

2. PURPOSE AND OBJECTIVES

2.1 Purpose

The purpose of the Mandeni Local Municipality Change Control Policy is to establish a formal and consistent approach for managing, controlling, assessing, approving, implementing, and monitoring changes to the Municipality's ICT environment.

The policy is intended to minimise the risks associated with ICT changes, including system disruption, service outages, data loss, security vulnerabilities, configuration errors, failed implementations, and non-compliance.

The policy ensures that changes are introduced in a controlled, documented, risk-based, and auditable manner, while enabling the Municipality to respond effectively to business requirements, technological developments, cybersecurity threats, incidents, and operational needs.

The policy supports the Municipality's ICT governance and cybersecurity objectives and aligns change management practices with COBIT 2019, particularly BAI06 – Managed IT Changes, which focuses on managing and controlling changes throughout their lifecycle.

2.2 Objectives

The objectives of the Change Control Policy are to:

- Ensure all ICT changes are formally requested, documented, assessed, and approved.
- Minimise disruption, downtime, and operational risks resulting from ICT changes.
- Ensure changes are appropriately tested and validated before implementation.
- Prevent unauthorised or uncontrolled changes to the Municipality's ICT environment.
- Ensure appropriate risk and impact assessments are conducted before changes are implemented.
- Ensure changes have appropriate rollback or recovery plans where required.
- Establish clear roles, responsibilities, and accountability for managing changes.
- Ensure emergency changes are controlled, documented, and reviewed.
- Maintain an accurate Change Register and audit trail.

- Ensure changes that may affect cybersecurity and information security controls are appropriately assessed.
- Monitor change management performance and promote continuous improvement.

3. POLICY PRINCIPLES

3.1. All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria.

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

3.3. Implementation will only be undertaken after appropriate testing and approval by stakeholders.

3.4. 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.

3.5. All changes will be monitored once they have been rolled-out to the production environment.

4. CHANGE CONTROL POLICY

Changes to information resources shall be managed and executed according to a formal change control process. This control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in controlled manner; and that the status of each proposed change is monitored.

In order to fulfil this policy, the following statements shall be adhered to.

4.1. Change Control

4.1.1. Corrections, enhancements and new capabilities for applications and infrastructure will follow a structured change control process.

4.1.2. An emergency change must follow a structured change control process, but with the understanding that documentation must be completed afterwards.

4.1.3. Recurring change requests from users (e.g. user access requests, a password reset, an installation, move or change of hardware and software etc.) must follow the processes designed to deliver ICT services in the most effective way.

4.1.4. Systems must have a development environment where testing is conducted to avoid testing in the production environment.

4.2. Directives

4.2.1. All changes shall be recorded, initiated, controlled and implemented within the documented change management process. There will be no exception to this directive, unless duly authorised.

4.2.2. In the event of a major emergency, ICT back end changes shall be classified and managed according to the change management process. For as long as such changes will not have effects on how end users discharge their work.

4.2.3. All those who attend the presentations and workshops for this policy shall confirm their attendance on the provided attendance register. Signing the attendance register confirms understanding the contents of this policy and acknowledging this policy.

4.2.4. All members of the MLM shall read and ensure they understand this policy.

4.3. Change Analysis

4.3.1. Change records must be analysed regularly to detect increasing levels of changes, frequently recurring types, emerging trends and other relevant information. Changes to production Information Resources must be documented and classified according to their importance, urgency, impact, and complexity.

4.3.2. The result and conclusions from ICT change analysis shall be recorded.

4.3.3. Action for improvement identified from change management shall be recorded and input into a Service Improvement Plan (SIP) for improving the service.

4.4. Implementation

4.4.1. Implementation will only be undertaken after appropriate testing and approval by ICT Steering Committee. Major changes will be classified according to effort required to develop and implement said changes.

4.5. Change Classification

4.5.1. All changes need to be classified according to how much impact they will have on the Municipality and service provision. These changes will all have different priorities based on assessed urgency and impact levels.

4.6. Roll Back Planning

4.6.1. All changes must be approved and implemented in a controlled manner and according to the documented process.
4.6.2. All changes shall be reviewed for success and any actions taken after implementation.
4.6.3. A forward schedule of changes that contain details of all the changes approved for the implementation and their proposed implementation dates shall be maintained and communicated to relevant parties.

4.7. Change Approval

4.7.1. All changes shall be approved by the ICT Steering Committee.
4.7.2. ICT Manager shall at all possible times inform users on all the technical changes through written email or any other form of communication. Others may need to be consulted.
4.7.3. ICT Steering Committee may delegate and/or pre approve some recurring changes provided that the ICT Steering Committee will regularly review those changes.

4.8. Risk Management

4.8.1. A risk management shall be performed for all the changes and dependant on the outcome, an impact assessment shall be performed.

4.9. Document Change

4.9.1. All changes requests shall be logged whether approved or rejected on a standardised and central system. This should include change request documentation, authorisation and the outcome of the change. No single person should be able to effect changes to production information system without the approval of the other authorised personnel.

5. POLICY ENFORCEMENT

5.1. Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

5.2. Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

6. RESPONSIBILITIES

6.1. The ICT Manager is responsible for:

6.1.1. Change request and potential risks and introduce counter measures to address these risks.

6.1.2. Approve and authorise change control procedures.

6.1.3. Ensure that policy, standards and procedural changes are communicated to applicable users and management.

6.1.4. Facilitate and coordinate the necessary change management procedures within the Municipality.

6.1.5. Review the effectiveness of change management strategy and implement remedial controls where deficits are identified.

6.2. The ICT Steering Committee shall ensure that the necessary information security controls are implemented and complied with as per this policy.

6.3. The ICT division is responsible to make sure that they are keeping changes in compliance with this Change Control Policy. It is the responsibility of every user of ICT Infrastructure to ensure adherence to this Change Control Policy.

7. POLICY MAINTENANCE

7.1. User and administrator activity must be monitored through audit and event logging.
7.2. All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes.
7.3. Log must be reviewed monthly for specious or malicious activities.
7.4. A change that affects only a single user will need verbal approval from ICT Manager.

8. NON-COMPLIANCE

Where non-compliance is found, necessary steps will be taken to remedy the situation. The remedy may include actions as per the Mandeni Local Municipality's Disciplinary Code and could lead to dismissal.

9. PERFORMANCE METRICS

The effectiveness of the Change Control Policy shall be measured through the following KPIs:

Table 2: KPIs

KPI	Target	Frequency
Percentage of changes formally logged in the Change Register	**100%**	Monthly
Percentage of changes approved before implementation	**100%**	Monthly
Percentage of changes with documented impact and risk assessments	**100%**	Monthly
Percentage of applicable changes tested before production implementation	**≥95%**	Monthly
Percentage of changes implemented according to approved implementation plans	**≥95%**	Monthly

KPI	Target	Frequency
Percentage of changes with documented rollback/back-out plans	**100% for applicable changes**	Monthly
Percentage of successful changes	**≥95%**	Monthly
Percentage of failed changes	**≤5%**	Monthly
Percentage of emergency changes retrospectively reviewed	**100%**	Monthly
Percentage of emergency changes appropriately documented	**100%**	Monthly
Number of unauthorised changes identified	**0**	Monthly
Percentage of unauthorised changes investigated and remediated	**100%**	Monthly
Percentage of high-risk changes reviewed by the appropriate Change Authority/CAB	**100%**	Monthly
Percentage of significant changes subjected to post-implementation review	**100%**	Monthly
Percentage of change-related incidents resolved and linked to the relevant change record	**100%**	Monthly
Percentage of changes resulting in service disruption	**≤5%**	Monthly
Percentage of change records containing complete supporting documentation	**≥95%**	Monthly
Percentage of change-related audit findings closed within agreed timelines	**≥95%**	Quarterly
Percentage of ICT personnel and relevant third parties complying with change control procedures	**≥95%**	Quarterly
Change Control Policy and procedures reviewed and updated	**100%**	Annually

10. APPENDICES

APPENDIX A_Change Management Process

APPENDIX B_Change Request Form.docx

11. POLICY REVIEW & APPROVAL

This policy shall be reviewed on an annual basis by the ICT Manager to determine if there are improvements or changes in the ICT process that should be reflected in this policy.

This document becomes effective upon approval by the Municipal Manager and Council as required.

PREPARED BY: P.E. NTANZI

DATE OF ADOPTION BY COUNCIL: 30 JULY 2026

COUNCIL RESOLUTION NO: C22

30/07/2026

MUNICIPAL MANAGER

DATE

S.G. KHUZWAYO