-
-
-
-

BELA-BELA LOCAL MUNICIPALITY

Chris Hani Drive, Bela- Bela, Limpopo. Private Bag x 1609
BELA-BELA 0480
Tel: 014 736 8000 Fax: 014 736 3288
Website: www .belabela.gov.za

-

- OFFICE OF THE MUNICIPAL MANAGER

Information and Communication Technology

Change Management Policy and Procedure

TABLE OF CONTENT

POLICY AUTHORITIES

Compiled by	D Nkuna
Designation	Divisional Manager IT
Signature	
Date	
Supported/Not Supported	ML Mashishi
Designation	Acting Corporate Services Manager
Signature	
Date	
Approved/Not Approved	MM Maluleka
Designation	Municipal Manager
Signature	
Date	
Effective Date	

POLICY CHANGE RECORD

The following changes have been made to this policy:

Version	Description of Change	Date Approved

1. MANDATE OF THE ICT DIVISION

1.1 The Information and Communications Technology (ICT) Division has the mandate to deliver services, support and maintain ICT infrastructure, for the Municipality to realise its mandate.

2. OBJECTIVE OF THE POLICY

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

3. APPLICABILITY OF THE POLICY

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

4. ACRONYMS

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

5. REFERENCES

5.1 International Guidelines

a. Control Objectives for Information Technology (COBIT)

5.2 International Standards

b. Information Technology Infrastructure Library (ITIL)

c. ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management

5.3 National Policy

d. Constitution of the Republic of South Africa, Act 108 of 1996

f. The Electronic Communications and Transactions (ECT) Act 25 of 2002

g. National Strategic Intelligence Act 2 of 2000 applicable for South Africa

h. Regulation of Interception of Communications Act 70 or 2002

i. State Information Technology Act 88 of 1998.

6. PRINCIPLES

6.1 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

c. Exposure to reputational risk

7. APPLICATION

7.1 Procedure

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 procedures). This process shall include management responsibilities and procedures. Wherever practical, operational and application change management procedures 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

7.2 Documented Change

a. All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

b. The ICT Division shall maintain a documented audit trail, containing relevant information at all times. 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.

7.3 Risk Management

a. A risk assessment shall be performed for all changes and depending on the outcome, an impact assessment should be performed.

b. 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.

7.4 Change Classification

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

7.5 Testing

a. 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.

7.6 Changes Affecting Service Level Agreements

a. 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.

7.7 Version Control

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

7.8 Approval

a. 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.

7.9 Communicating Changes

a. 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.

7.10 Implementation

a. 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.

7.11 Fall Back

a. Procedures 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), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures shall be in place to ensure systems can revert back to what they were prior to implementation of changes.

7.12 Documentation

a. 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.

b. 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 procedures, affected by software changes, shall be updated on completion of each change.

7.13 Disaster Recovery Plan (DRP)

a. 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.

7.14 Emergency Changes

a. Specific procedures 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.

7.15 Change Monitoring

a. 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.

8. ROLES AND RESPONSIBILITIES

8.1 The Change Committee shall:

a. Ensure that the necessary information security controls are implemented and complied with as per this policy

8.2 The ICT Manager shall:

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

8.3 The ICT Manager shall:

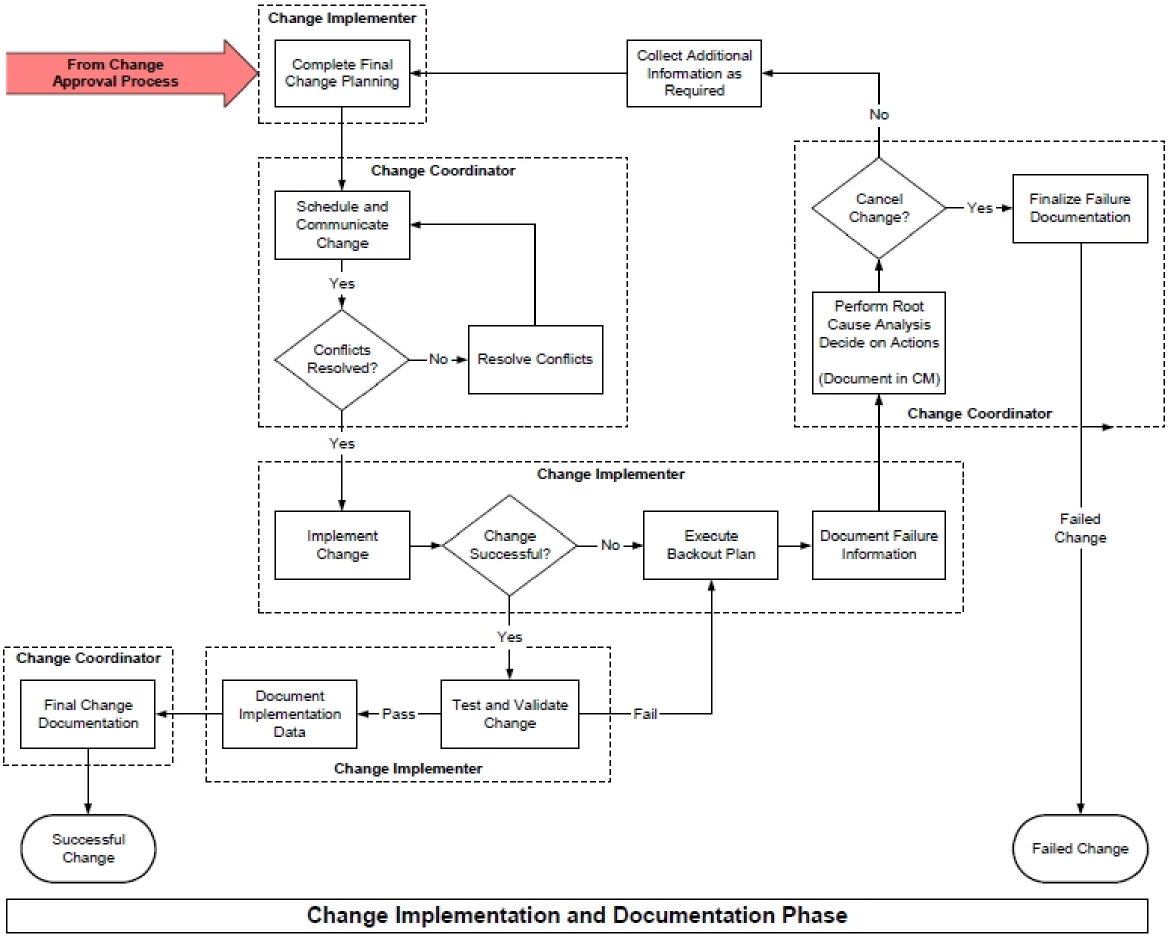
a. Establish and revise the information security strategy, policy and standards for change management

b. Evaluate incidents and potential risks to the Municipality and facilitate the necessary counter measures to change management initiatives and evaluate such policies and standards

c. Coordinate the overall communication and awareness strategy for change management

d. Coordinate the implementation of new or additional security controls for change management

9. Change Management Work Flow


From Change Approval Process
Change Implementer
Complete Final Change Planning
Collect Additional Information as Required
No
Change Coordinator
Schedule and Communicate Change
Yes
Conflicts Resolved?
No
Resolve Conflicts
Yes
Cancel Change?
Yes
Finalize Failure Documentation
Perform Root Cause Analysis Decide on Actions (Document in CM)
Change Coordinator
Change Implementer
Implement Change
Change Successful?
No
Execute Backout Plan
Document Failure Information
Failed Change
Yes
Change Coordinator
Final Change Documentation
Document Implementation Data
Pass
Test and Validate Change
Fail
Change Implementer
Successful Change
Failed Change
Change Implementation and Documentation Phase

POLICY REVIEW

10.1 This policy shall be reviewed on an annual basis by the ICT Manager to:

a. Determine if there have been changes in International, National or Internal references that may impact on this policy.

b. Determine if there are improvements or changes in the ICT process that should be reflected in this policy.