Okhahlamba Local Municipality

ICT Change Management Policy

Policy Reference Number	
Version Number	*0.1*
Effective Date	
Review Date	*One year after Effective Date*
Policy Owner	*Thami Makhubu* *IT Officer*
Signature	
Policy Sponsor	*Gugu Mohlakoana* *Director Corporate Services*
Signature	
Date Approved	

Stakeholders

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Compulsory Stakeholder Involvement						
Subject Matter Experts						
Risk Management						
Compliance						
Legal Services						
Other Stakeholder Involvement						
Human Capital (Incl. Labour Consultation)						
ICT						
"Other"(Please specify)						

Recommended by Procedure Owner and Procedure Sponsor:

I hereby acknowledge that a search has been conducted and that the Policy is not duplicated or in conflict with any other Okhahlamba Municipality Policies.

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Policy Owner						
Policy Sponsor						

Final Approval

_____

Name of Committee

_____

Date Approved

Summary of Version Control

Version Number	Effective Date	Summary of Changes
0.1	TBD	First Draft

Table of Contents

1 Background 6
2 Purpose 6
3 Definitions 6
4 Scope 6
4.1 Activities 6
4.2 Audience 7
4.3 It Services 7
4.4 Activities Out Of Scope 7
5 Policy Statements 7
5.1 General 7
5.2 Emergency Changes 8
5.3 Change Advisory Board (CAB) 8
5.4 Emergency Change Advisory Board (ECAB) 9
5.5 Change Freeze Periods 9
5.6 Cancelling a change 9
5.7 Post Implementation Review of Changes 10
5.8 Change Record Closure 10
5.9 Unauthorised Changes 10
6 Roles And Responsibilities 10
7 Related Information And Reference 10
7.1 Internal Documents: 10
7.2 External Documents: 10
7.3 Regulatory Requirements: 11
8 Financial Implications 11
9 Exclusions 11
10 Request To Deviate From Policy 11
11 Compliance Monitoring 11
12 Non-Compliance 11

1 BACKGROUND

Change Management's (CM) function is to ensure that modifications to the Okhahlamba Municipality ICT environment are recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner to minimise the risk of negative impact of changes to Okhahlamba Municipality.

This policy governs changes made to all Okhahlamba Municipality ICT, Service Components (SC) and Configuration Items (CIs). This includes but is not be limited to:

- Host systems, including rebooting of servers;
- Environmental components, power systems, fire suppression systems;
- All hardware components;
- Software elements including application and databases systems;
- Network components including physical cabling;
- Security devices; and
- Documentation including policies, procedures, service catalogues, and system documentation.

2 PURPOSE

This policy document establishes the principles and practices for ICT Change Management within Okhahlamba Municipality. How these principles and practices are implemented is set out within a separate, but supporting, Procedures document.

3 DEFINITIONS

Definitions for terms which are capitalised can be found in a separate glossary which applies to all ICT Policies, Standards and Procedures documents and related documents.

4 SCOPE

4.1 ACTIVITIES

Change Management's key activities include ensuring that all changes to all environments are: recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed. Change Management is also responsible for reporting on the effectiveness of the process to senior management and identifying improvements that can be made. Ensuring that the Change Management process is auditable and key risks have been identified and mitigated against.

4.2 AUDIENCE

1. ICT staff whose job role(s) include:
   - Making changes to existing ICT Services, Service Components (SC) and Configuration Items (CIs);
   - Delivering and supporting Services;
   - Supporting deployed Services; or
   - Representing IMS to the Business; or
   - Any other responsibilities where awareness of the Policy is necessary.
2. Municipal personnel who:
   - Represent Municipality's interests as the recipient of deployed Services.

4.3 IT SERVICES

This Policy applies to all ICT Services within the Municipality.

4.4 ACTIVITIES OUT OF SCOPE

The scope of Change Management covers changes to Services and Configuration Items across the entire Service Life Cycle as dictated by Configuration Management

Changes that lie outside the scope of the ICT Change Management process include:

- Organisational changes;
- Changes to business operations; and
- Changes at an operational level such as repair to printers or other routine service components.

5 POLICY STATEMENTS

5.1 GENERAL

1. Okhahlamba Municipality will adopt a common Change Management Process for handling and controlling ICT changes throughout the Municipality.
2. Change Management Process activities will be documented in a Procedures document.
   - The Process and their activities will conform to ITIL and COBIT Best Practice, allowing for some minor differences to enable customisation to Okhahlamba Municipality's environment.
   - Appropriate customisation to the common Change Management Process activities is permitted.
3. All Changes will follow the Change Management Process. This includes those for Services supported by Vendors.
4. The IT Officer will manage all Changes in such a way to minimise impact to the Municipality.
5. The IT Officer records will be audited to ensure that the information in them is accurate and complete.
6. The IT Officer will identify improvement opportunities and include them in the Continual Service Improvement register.

7. The IT Officer will define relevant process KPIs, and track and report on them to Management.
8. Management will ensure that sufficient resources are allocated to execute Change Management effectively and efficiently.
9. All Requests for Change will be recorded and managed in an IT Service Management Tool. If an IT Service Management Tool has not been implemented manual processes will be used until a tool is implemented.
10. All Changes records will be updated with relevant and complete information so as to record a full history. This will include, but not be limited to:
    - Requests for Change form.
    - Risk Assessment of the change;
    - A Test Plan.
    - Implementation Plan.
    - A Back-out Plan.
    - Communication Plan.
    - ICT Incident Management report.
    - ICT Problem Management report.
    - Post Implementation review report.
11. All submitted Requests for Change will be evaluated for completeness by the IT Officer.
12. Incomplete forms will **not** be submitted to the Change Advisory Board (CAB) for approval;
13. The Change Advisory Board (CAB) will authorise RFCs based upon the risk assessment, service levels and provided there is a business justification for the change.
14. Testing must be performed in an appropriate testing area and not on the production environment.
15. All Changes to existing Configuration Items (CIs) that are not yet in the CMDB, must be added to the CMDB in conjunction with their maturation of the Change Process.
16. Some incidents may or not may not be related to a Change, but where a Change has caused an incident then it will be possible to trace this back to the person responsible for make that change. The IT Officer will facilitate a review meeting and a report will be generated and fed back to the Change Advisory Board.

5.2 EMERGENCY CHANGES

1. An Emergency Change is a change that must be introduced as soon as possible as the result of an urgent or critical event. This event must have significant impact on ICT services. Each situation is different and as much consideration as possible should be given to the possible consequences of attempting this type of change. Emergency Changes must be authorised by the Emergency Change Advisory Board (ECAB). Full documentation must be submitted to the CAB upon abatement of the crisis. A RFC for the Emergency Change must be created within a reasonably timeframe within 24 hours after the change. The Post Implementation Review report for the Change must be submitted within a 3 days after the emergency change.

5.3 CHANGE ADVISORY BOARD (CAB)

1. The Change Advisory Board (CAB) reviews all RFCs submitted and determine whether or not they should be implemented. In addition, it may determine that certain changes are altered before implementing in order for it to be accepted.
2. The CAB will meet monthly. The IT Officer will provide an agenda of newly submitted items and a change status schedule. The purpose of this meeting will be to:
    - Bring all required parties together to assess the feasibility of implementing the change and provide status.
    - To review the status of all open changes and schedule for the current and upcoming weeks.
    - Discuss high impact changes.
    - Approve or disapprove each change as well as the Change Schedule.
3. Attendees of these monthly meetings are will be at least be the following:
    - IT Officer;
    - IT Assistant;
    - IT Security representative;
    - Vendor representatives.
    - CFO
    - Director for Social
    - Internal Audit

5.4 EMERGENCY CHANGE ADVISORY BOARD (ECAB)

1. We appreciate that due to the nature of these types of changes that it is not very practical to either wait for group of advisory board members to gather or to seek approval for a change to be made. This is made especially difficult for out of hour's incidents that require immediate or quick changes to be made in order to restore a service. In these circumstances, the IT Officer, IT Assistant and representatives from the business units that will be affected by the Change have the authority to approve a change. It is acknowledged that in some exceptional circumstances that this may not be possible and the authority will then fall on the person making the change. However, the change request form should still be filled in, even if it is retrospectively.

5.5 CHANGE FREEZE PERIODS

1. At certain critical times of the year, it will be necessary to impose a non-essential change freeze period. During this time you should only make changes that are deemed essential to either the running of or fixing of a problem with a particular service. If you have the need to make a change during this time, then please follow the instructions sent out with the change freeze dates. If in doubt, contact the IT Officer. The dates of any change freeze will be communicated well in advance so that you are enable to plan your work around them.

5.6 CANCELLING A CHANGE

1. If for any reason a CAB-approved change has to cancelled or postpone, then the IT Officer has to be informed.

2. If the Change will need to be performed at a later date then a new RFC must be submitted.

5.7 POST IMPLEMENTATION REVIEW OF CHANGES

1. After any change has been implemented, the person who is responsible for implementing the Change will perform a Post Implementation review of the Change. This report will be included as part of the Change Record and will be submitted to the CAB.
2. The CAB will perform a review of all detailed review of all unsuccessful Changes to determine the why the change was not implemented as planned. The results of the review will be stored in a lessons-learned repository and used for process evaluation and continual process improvement.

5.8 CHANGE RECORD CLOSURE

1. Before a Change record is Closed, the following quality assurance will be done:
   - Verification that the Change was implemented as planned.
   - If the Change was not implemented as planned then the reasons for this will have been documented in the Post Implementation Review. Unsuccessful Changes will have to be closed and be resubmitted as a new Change after the requestor of the change has satisfied the CAB that the causes of the unsuccessful initial implementation have been addressed.

5.9 UNAUTHORISED CHANGES

1. Unauthorised Changes are a serious breach of this policy and an unacceptable risk to Okhahlamba Municipality. If unauthorised changes are detected the CAB will sanction an investigation to determine the impact of the unauthorised Changes and what actions need to be taken.

6 ROLES AND RESPONSIBILITIES

7 RELATED INFORMATION AND REFERENCE

This Policy should be read in conjunction with the following supporting guidelines:

7.1 INTERNAL DOCUMENTS:

- IT Security Policy

7.2 EXTERNAL DOCUMENTS:

- ITIL Service Design, 2011 edition
- COBIT 5 Enabling Processes (2012)

7.3 REGULATORY REQUIREMENTS:

Okhahlamba Municipality recognises the importance of complying with all applicable regulatory requirements.

8 FINANCIAL IMPLICATIONS

None.

9 EXCLUSIONS

There are no exclusions to this Policy.

10 REQUEST TO DEVIATE FROM POLICY

In cases where material and compelling circumstances merit deviation(s) from particular provision(s) of this Policy, written submissions shall be sent to IT Officer, who shall have full authority to grant such request, in whole or in part, or to refuse same.

11 COMPLIANCE MONITORING

The IT Steering Committee will be accountable for compliance monitoring.

12 NON-COMPLIANCE

Breaches of this Policy will be seen in a very serious light. Employees who do not conform to the Policy or Procedures & Standards may be subject to disciplinary action in terms of the applicable Okhahlamba Municipality disciplinary processes and procedures.