UPHUHLISO LWABANTU KUQALA

INGQUZA HILL
LOCAL MUNICIPALITY

ICT CHANGE MANAGEMENT MANUAL

TABLE OF CONTENTS

1. ABBREVIATIONS AND DEFINITIONS

Throughout this document various acronyms, abbreviations and definitions are referred to. For the purpose of this Change Management document these are defined as follows:

AG	Auditor General
CoBit	Control Objectives for Information and Related Technology
IHLM	Ingquza Hill Local Municipality
DRP	Disaster Recovery Plan
MM	Municipal Manager
IS	Information System
ISF	Information Security Forum
ISO	Information Security Officer
ISS	Information System Security
IT	Information Technology
ITIL	Information Technology Information Library
KPA	Key Performance Area
KPI	Key Performance Indicator
MISS	Minimum Information Security Standard
OLA	Operational Level Agreement
MFMA	Municipal Finance management Act
POPI	Protection of Private Information Bill
PSR	Public Service Regulations
SLA	Service Level Agreement
CAB	Change Advisory Board
RFC	Request For Change

2. BACKGROUND AND INTRODUCTION

The intention of an ICT policy is to provide guidelines for the use of the electronic media and where abuse occurs, sets out the punitive measures that can be taken against an employee. The ICT policy also specifies the security measures and safeguards that should be applied by the IT department and the employees alike.

Define guidelines, standards and procedures for INGQUZA HILL LOCAL Municipality divisions providing information or services on the Internet. Therefore this manual seeks to address the following;

Change Management is the process of planning, coordinating, implementing and monitoring changes affecting any production platform within Information Technology's control.

3. PURPOSE

The purpose of the Change Management Manual is to provide a comprehensive plan on how to manage changes, particularly IT related changes, in a rational and predictable manner so that staff and clients can plan and adjust accordingly with as minimum disruptions to the operations of the municipality as possible. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

4. OBJECTIVES

The objectives of the Change Management procedure manual are to:

a) Ensure that changes are made with minimum disruption to the services IT has committed to its users;
b) Support the efficient and prompt handling of all changes;
c) Provide accurate and timely information about all changes;
d) Ensure all changes are consistent with business and technical plans and strategies;
e) Ensure that a consistent approach is used;
f) Ensure all ICT changes are evaluated, prioritized and authorized;
g) Ensure all types of ICT changes, including emergency changes are managed effectively;
h) Ensure that the status of ICT change requests are tracked and reported;
i) Provide additional functionality and performance enhancements to systems while maintaining an acceptable level of user services;
j) Reduce the ratio of changes that need to be backed out of the system due to, inadequate preparation;
k) Ensure that the required level of technical and management accountability is, maintained for every change;
l) Monitor the number, reason, type, and associated risk of the changes.

5. SCOPE

This, the IHLM Change Management Procedure manual, applies to all individuals that install, operate or maintain Information Resources within the municipality.

It includes the management of any installation or alteration to hardware, network, system or application software, procedure or environmental facilities which adds to, deletes from or modifies the service delivery environment.

6. ROLES AND RESPONSIBILITIES

6.1. IT Manager

The IT Manager shall implement, enforce and monitor the change controls in accordance with the requirements outlined in this manual, and must advise users on the correct ways to access the changed or changing state in information and/or systems.

6.2. All Employees

All employees are responsible for complying with this change management procedure manual at all times. This manual also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour).

6.3. Information Systems Owners

This is the custodian user or administrator wherein the change is being effected. This System Owner is responsible for analysing key change elements, documenting them and submitting to the IT Manager for consideration. This system owner forms part of the committee approving all changes that affect the system they are responsible for.

6.4. System Administrator

The system administrator is responsible for maintaining this procedure manual and advising the IT Manager on proposed amendments, additions or omissions as technology evolves. The System Administrator will be generally advising on information security controls. Working in conjunction with other department functions, is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this manual.

6.5. Internal Audit

The Internal Audit unit is authorised by management to assess legislative and corporate governance compliance with this and all municipal policies.

7. POLICY STATEMENTS

a) Every change to IHLM Information Resources such as:
   - operating systems;
   - computing hardware
   - networks;
   - and applications is subject to the Change Management Manual and shall be performed according to the Change Management Procedures;

b) The change management procedure shall ensure that proposed changes are reviewed for relevancy and impact (business, technical and financial);

c) The change management procedure will be formally defined, documented and adhered to;

d) All changes affecting computing environmental facilities (e.g., air-conditioning, water, fire and electricity) need to be reported to or coordinated with the leader of the change management process;

e) IHLM ICT Change Management Committee shall be appointed by the MM and will be responsible to review change management requests as an item to ensure that change reviews and communications are being satisfactorily performed,

f) A formal written change request shall be submitted for all changes, both scheduled and unscheduled;

g) All scheduled change requests shall be submitted in accordance with change management procedures so that the ICT Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request;

h) Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change,

i) The appointed leader of the Change Management Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available;

j) Changes are to be fully tested in an isolated, controlled and representative environment, and approved before being implemented;

k) Any software change and/or update will be controlled with version control,

l) Using live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place;

m) Data is to be protected against unauthorised or accidental changes;

n) Fallback procedures for aborting and recovering from unsuccessful changes will be documented and tested;

o) Emergency changes will be authorized and recorded;

p) Disaster recovery plans will be updated with relevant changes and managed through the change control process. Change request will be utilized as evidence of change should the change affect SDBIP project targets. These records may also be used as evidence to AG;

q) Information resources documentation will be updated when each change is complete and old documentation will be archived or disposed of according to the documentation and data retention policies;

r) Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures;

s) A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not;

t) A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
   - Date of submission and date of change
   - Owner and custodian contact information
   - Nature of the change
   - Indication of success or failure.

u) All IHLM information systems must comply with an Information Resources change management process that meets the standards outlined above;

v) The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data;

w) All changes or modifications to IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.

x) The access of the programmer to the production environment is only through approval of the IT Manager (for routine checks) and CAB for changes.

8. CATEGORISATION OF ICT CHANGES

a) All non-routine ICT changes must be categorised according to their impact and their urgency;

b) Where applicable, the service level agreement of an ICT service can help determine the urgency;

c) The following scale must be used to determine the impact of an ICT change:

LEVEL	POTENTIAL IMPACT
Level 5	Critical impact on the whole IHLM operation.

Level 4	Significant impact on the whole IHLM operation or critical impact on a group of users.
Level 3	Mild impact on the whole IHLM operation, significant impact on a group of users or critical impact on one user.
Level 2	Mild impact on a group of users, significant impact on a user.
Level 1	Mild impact on a user.

d) The following scale must be used to determine the urgency of an ICT change:

LEVEL	**URGENCY**
Level 5	Immediate (Emergency Change).
Level 4	1 week.
Level 3	2 weeks.
Level 2	1 month.
Level 1	At convenience.

9. ROUTINE CHANGES

A routine change is an ICT change that forms part of a standard operational procedure and has an impact of level 2 and subscribes to the below prescripts:

a) The routine change procedure must be documented and must form part of a pre-approved list of routine changes;
b) The list of routine changes must include a description of the change, who is allowed to make the change, a reference to the standard operational procedure and a roll back procedure if required;
c) A routine change is well known, the solution is well tested and the risk involved to the ICT environment is minor;
d) Examples of routine changes include adding a new user to an information resource, removing a user from an information resource, changing a password, anti-virus updates and service pack updates.

10. MINOR CHANGES

A minor change is defined as any ICT change with an impact that is level 2 and below and an urgency that is level 4 and subscribes to the prescripts below:

a) A Request For Change (RFC) must be submitted to the service desk for a minor change;
b) A minor change must be approved by the ICT Infrastructure manager and the CAB notified beforehand of the proposed ICT change. The CAB may reject the change if they consider it too risky or change the impact or urgency rating;
c) A minor change does not need formal CAB approval, but the ICT change must comply with all aspects of the ICT change management process;

11. MAJOR CHANGES

A major change is defined as any ICT change with an impact that is level 3 and above and is not deemed to be an emergency change:

a) An RFC must be submitted to the service desk for a major change;
b) A major change must be formally approved at a sitting of the CAB and must comply with all aspects of the ICT change management process.
c) Upon successful changes in the environment the UAT must be signed attached as Annexure A herein.

12. EMERGENCY CHANGES

An emergency change is an ICT change that requires an immediate response (level 5 urgency) in order to minimise the impact to the IHLM and to prevent widespread service disruption:

a) An emergency change must be the exception to the norm and selected with caution;
b) An emergency change must be approved by the ICT infrastructure manager and the CAB notified beforehand of the proposed ICT change;
c) After the emergency change has been implemented, an RFC must be submitted by the ICT infrastructure manager to the service desk in order to track emergency changes;
d) A formal process must be documented for dealing with emergency changes to ensure the risk of poorly executed changes are minimized as far as possible.
e) A formal report must be submitted for all emergency changes including:
    - Who discovered the need for an emergency change;
    - Description of the need for the emergency change and how it was discovered;
    - The justification for the emergency change made; why it was classified as an emergency change.
f) What analysis was made to uncover the impact and urgency of the emergency change;
g) What was the roll-back for the emergency change, if any;
h) How the emergency change was executed.
i) What the emergency change accomplished (solution/positive effects).
j) What was the negative consequences resulting from the change.

13. NON-ADHERENCE

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UHLM access privileges, civil, and/or criminal prosecution.

14. COMMENCEMENT OF THE PROCEDURE MANUAL

- The policy will come into effect on the date signed by ICT Governance Champion

14.1. INTERPRETATION OF THE MANUAL

- All words contained in this policy shall have the ordinary meaning attached thereto, unless the definition or context indicates otherwise
- Any dispute on interpretation of this policy shall be declared in writing by any party concerned.
- The Municipal Manager shall give a final interpretation of this policy in case of written dispute.
- If the party concerned is not satisfied with the interpretation, a dispute may then be pursued with the South African Local Government Bargaining Council.

15. PERMANENT/TEMPORAL WAIVER OR SUSPENSION OF THE MANUAL

- This manual may be partly or wholly waived or suspended by the ICT Governance Champion on temporary or permanent basis however the Municipal Manager/Council may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to Council

16. COMPLIANCE AND ENFORCEMENT

- Senior management is required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
- Failure to comply with this policy may result in disciplinary action, which may include termination of employment.
- Any conduct that interferes with the normal and proper operation of the municipality's IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.
- The municipality management reserves the right to revoke the privileges of any user at any time.

17. AMENDMENT AND/OR ABOLITION OF THIS MANUAL

- This manual may be amended or repealed by ICT Governance Champion /Council as it may deem necessary.

17.1. ANNEXURE A: USER ACCEPTANCE SIGN-OFF

Use this form for all projects/tasks/systems/scripts/etc. that need to move to production and /or have gone before the CAB. This document should be filled out and signed by the appropriate party

SECTION A: INITIATOR/REQUESTOR INFORMATION			
Project Name		**Date**	

Function or Task		**Module**	
SECTION B: PROJECT TEAM INVOLVED			
CORE TEAM INVOLVED		**SECONDARY TEAM INVOLVED**	
List Name And Department (Be Specific)		*List Name And Department (Be Specific)*	
TESTED BY		**TESTED ON**	
List Name And Department (Be Specific)		*List Platform the Change was tested on (Be Specific)*	
PROOF OF COMPLIANCE		□ User Acceptance Checklist completed and attached □ Test Results attached □ Outstanding issues with resolution plans attached	
COMMENTS			

18. KEY REFERENCES

The document has been drafted with particular reference to:

1. The Promotion of Access to Information Act, 2000 (Act no. 2 of 2000)
2. The Protection of Information Act, 1982 (Act no. 84 of 1982)
3. SABS/ISO 17799

4. Minimum Information Security Standards (MISS)
5. Guidelines for the Handling of Classified Information (SP/2/8/1)
6. Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)

19. APPROVAL

The signatories hereof, being duly authorized thereto, by their signatures hereto authorize the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorize the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

Signature:

01/03/2017
Date:

MUNICIPAL MANAGER
Position