DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

INFORMATION COMMUNICATION TECHNOLOGY(ICT) CHANGE MANAGEMENT POLICY

ICTCMP - VERSION 1.2
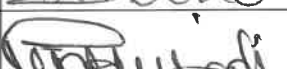
Document Details

Author	Directorate Information Communication Technology
Department	Community Safety and Transport Management
Division Name	ICT Management
Document Name	Information Communication Technology Change Management Policy
Sensitivity	Internal Use Only
Effective Date	After the Accounting Officer 's signature
Created Date	23-07-2018
Version Date	<date of Accounting Officer signature>

Change Record

Modified Date	Author	Version	Description of Changes
31 – 01 - 2019	Director Information Communication Technology	1.1	Changes in the Departmental environment, address audit findings and alignment of policies
29-11-2021	Information Communication Technology	1.2	Review

Stakeholder Sign–Off

Name	Position	Signature	Date
Mr O. Gabonnwe	Departmental Information Technology Officer		21/02/2025
Ms K. Phatudi	ICT Governance Champion		21/02/2025
Mr T. Sematle	Chairperson: ICT Steering Committee		21/02/2025
Ms K. Phatudi	Chairperson: ICT Strategic Committee		21/02/2025
Ms M.G. Mothibedi	Chief Risk Officer		21/02/2025
Ms M. Mogatusi	Acting Director Legal Services		21/02/2025

Records Management Sign–Off

Name	Position	Signature	Date
Mr E. Khuto	Deputy Director Records Management		10/03/2025

TABLE OF CONTENTS

Glossary of Terms

Change Management	Is a systematic approach to dealing with the transition or transformation of the departmental goals, processes or technologies
Departmental ICT Steering Committee	The Committee responsible for evaluating and assessing change requests
RFC	Request for Change
DCSTM	Department of Community Safety and Transport Management
Department	Department of Community Safety and Transport Management
DITO	Department Information Technology Officer
HoD	Head of Department
Information Communication Technology (ICT)	The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
User	Employee accessing the system for the purpose of processing or authorising transaction, updating or amending system data or extracting Management reports from such system.

1. Introduction

This Policy is designed to document how Departmental ICT manages changes to Departmental Systems to minimize risk and impact to the department.

ICT Change Management can be defined as a process to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. ICT changes can be executed as a result of departmental mandates designed to increase efficiency, or reflect business or service improvement initiatives. ICT Change management is made up of several processes: planning, testing, communicating, scheduling, implementation, documenting, and evaluating.

2.   Regulatory and Guidance Framework

i. Public Service Act (Proclamation No 103 of 1994)

ii. Labour Relations Act, 1995 (LRA)

iii. Electronic Communication and Transaction Act 25 of 2000

iv. State Information Technology Agency Act 88 of 1998 (as amended by Act 38 of 2002)

v. Departmental ICT Security Policy

vi. Departmental ICT User Account Management Policy

vii. Departmental ICT Portfolio Management Framework

viii. Electronic Communications and Transactions Act (no. 25 of 2002)

ix. Communication –related information Act (Act no. 70 of 2002)

x. Public Service Regulation of 2016, Chapter 6, Section 96

xi. Copyright Amended Act 9 of 2002, Chapter 1, Section 11B

xii. Protection of Information Act (Act no 84 of 1982)

xiii. Public Finance Management Act No. 1 of 1999 as Amended by Public Finance Management Amendment Act, No. 29 of 1999

3. Scope of application

This policy applies to all employees in the Department as well as other stakeholders utilising the departmental ICT network or systems.

4. Purpose and Objectives

The purpose of this policy is to describe the responsibilities, policies, and procedures to be followed when a change is to be made in the Departmental ICT Systems.

The objective of ICT Change Management is to enhance awareness and understanding of the proposed changes across the department and ensure that all changes are made in a thoughtful way that minimizes negative impact to services.

5. Administration of the policy

Departmental Information Technology Officer (DITO) is responsible for monitoring and must ensure compliance to the implementation of this policy. The Department needs to establish the Departmental ICT Steering Committee where all changes shall be presented for recommendations.

6. Policy Content

It is the responsibility of Information Communication Technology to manage the System Development Life Cycle of all the Departmental ICT Systems. All the processes and procedures relating to change control and management are clealy defined in this document.

The following steps shall be followed:

6.1 Identify Change

ICT Change occurs to improve a process, a system, or an outcome. This also involves identifying the resources and people who shall facilitate and lead the change process. The ICT change can be requested for the following reasons:

- Resolving problems;

- User wants an addition or alteration to the agreed-upon deliverables for a project;

- Other activities that influence service delivery.

6.2 Plan for the change

ICT changes must have a clear description of the project's scope, budget, schedule, and plans to manage risks and changes. ICT Change Management Plan should document how the changes shall be proposed, monitored, and controlled.

There should be no change without evaluation and approval by the relevant departmental committee. The Departmental committee must ensure that the resources are made available and the project is completed according to schedule.

6.3 Change Logging Procedure

The User/ Project Manager must complete the ICT Request for Change Form (*Annexure A*). There have to be clear reasons as to why there is a need for change to be made.

6.4 Communicating Change

The user shall sign off the change request form. Users shall be required to make submissions and comments prior to the acceptance of the change. The changes have to be presented to the Departmental ICT Steering Committee (which serves as the ICT Change Management Forum) for recommendation.

6.5 Approval for Change

The ICT Steering Committee shall ensure that all the relevant information provided is correct and complete. Once the ICT Steering Committee is satisfied with the information provided for RFC, the recommendations of the Request for Change by the ICT Steering Committee shall be forwarded to the Accounting Officer for review and approval.

6.6 Testing

ICT changes shall be tested in an isolated environment (where such an environment is feasible) before implementation of changes to verify that only intended and approved changes are made to assess their impact on operations and security.

6.7 Implementation of ICT change

A detailed implementation plan shall be in place on how the changes are going to be implemented. Major changes shall be classified according to the effort required to develop and implement the said changes. In the event where the implementation of change shall affect normal departmental operations, all affected directorates shall be informed of the impact of change. The DITO shall coordinate all ICT activities for the successful implementation of change and ensure that all the resources are available.

6.8 ICT Change Review

The DITO shall convene a meeting with the relevant stakeholders to review the ICT Change Implementation. Once the review process is finalised, the change meeting shall resolve to close the change. Feedback on the success or failure of the ICT Change shall be communicated to the Departmental ICT Steering Committee after the planned completion time.

6.9 Migration of changes to production

The development of the back-out plan is essential to ensuring the effective recovery of data in the event of a failed change. The back-out plan is based on the technical impact analysis and the implementation plan. The implementing team shall ensure that the current data is saved on an external computing resource or drive before the changes are effected.

6.10 Roll Back Plan

Not all changes will go as expected. If one activity in the change process fails, the system must roll back to the previous consistent and working configuration. Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different from 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. Rollback procedures shall be in place to ensure systems can revert to what they were prior to the implementation of changes.

7. Classification of Change

All ICT changes must go to the Departmental ICT Steering Committee. Changes are classified according to the urgency of the change and the potential customer impact.

7.1 Standard Change

Standard Changes are pre-approved changes that are considered relatively low risk, are performed frequently, and follow a documented Change Management process. The proposed Standard change describes how the change and associated risks shall be managed. Once the Accounting Officer or Delegated official has approved the Standard Change, it can be carried out.

7.2 Emergency Changes

An emergency change is where the department needs to make an urgent change to resolve a high-priority or high-impact outage. The objective is to speed up the change process and execute it quickly. The Emergency change shall be approved by DITO.

8. Change Request information

8.1 ICT Infrastructure Change Request

ICT Infrastructure refers to collection of hardware, software, networks, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support Information Communication Technology.

The infrastructure change request must consider the following:

- Description of the environment within which the change is requested;
- Impact on technology, processes and standard operating procedures;
- Impact on skills and competency requirements;

- Purpose of the change requested;
- Risks associated with change requested

8.2 Application Software Change request

Application Software refers to a computer program designed to help users perform their activities, it includes database, word processors, Web browsers and spreadsheets. The application change request must consider the following:

- The name of the application in which the change is requested;
- Purpose of the system;
- Description of change;
- Business processes impact;
- Impact of not implementing change

9. Computing resources lifespan

The Department shall replace desktops/laptops every four to five years. The replacement provides employees with competitive technology, stronger security standards, reduced downtime, and enhanced support.

The implication flowing from the above means that the budget for computing resources will have to be made up of possible replacements and new acquisitions. This means that Supply Chain Management would need to make use of their asset inventory which will inform the number of likely replacements and costs. This provision does not necessarily provide automatic replacement of equipment over four (4) to five (5) years, but it will be subject to recommendation by ICT using a technical inspection report.

10. Technical Impact Analysis

This process is intended to evaluate and validate the technical feasibility, risk and effect a change will have on the production environment and end-user productivity. Review the technical completeness of the change plan, including assets changed, impact on start-up or shut down of systems, the impact of back-up requirements, and operating system requirements.

11. Risk Management

Risk assessment shall be performed for all changes.

12. Roles and Responsibilities

12.1 ICT Steering Committee shall:

- Review all ICT changes to be implemented;
- Make recommendations for the attention of the Accounting Officer;
- Ensure that all the necessary security controls are implemented and complied with as per this policy.

12.2 Departmental Information Technology Officer shall:

- Evaluate ICT change requests and potential risks and come up with mitigation plans to address risks;
- Ensure that the policy and procedural changes are communicated to users and management;
- Coordinate the implementation of new or additional security controls for change management;
- Communicate all changes in the ICT Change Management process, working together with the other directorates;
- Promote awareness on the importance of ICT Change Management processes.
- Approve the emergency changes.

12.3 System Administrator shall:

- Take proactive steps to ensure compliance with the policy by all stakeholders.
- Ensure that the documentation, testing, and implementation of change are complete.
- Communicate change with all stakeholders, to understand the needs and expectations, and explain the changes and impact.
- Facilitate the process of managing change requests.
- Modify user's roles and privileges.

12.4 Software Developer shall:

- Modify a system configuration.
- Develop, coding, scripting or programming a system or application.
- Patching and updating the operating system.
- Make changes to system or application functionality processes.
- Modify the security configuration of IT systems or applications.

13. Policy Compliance

A breach of this policy shall have severe consequences and shall be treated in terms of the departmental disciplinary code.

14. Related Policies

Effective implementation of this policy requires that it be read together with other Departmental policies.

15. Review

This policy shall be reviewed every three (3) years and/or when such a need arises. This policy shall remain valid until approval has been granted for the reviewed policy.
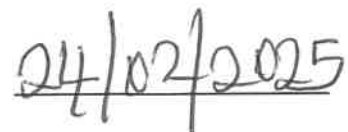
16. Approval

This policy is approved by the Accounting Officer and is applicable with effect from the date of approval below.

24/02/2025

DR H. KEKANA

DATE

ACCOUNTING OFFICER

INFORMATION COMMUNICATION TECHNOLOGY

Tirelo Building, Albert Luthuli Drive,
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735
Tel: +27 (18) 388 3697/ 5685

ICT REQUEST FOR CHANGE (RFC)   ANNEXURE A

General Information			
Requestor Name			Date
Office			
Contact Person	Phone	Email	Fax

Change Request Definition - (Fill in this section before the ICT Steering Committee requests an evaluation)

Description – Describe the proposed change.

Justification – Justify why the proposed changes should be implemented.

Impact of Not Implementing – Explain the impact if the proposed change is not implemented.

Change Request Evaluation Analysis (Fill in this section after ICT Steering Committee confirms evaluation is needed)

Check each that apply

☐ Project Schedule   ☐ Configuration Item   ☐ Product Deliverables affected

☐ Project Costs   ☐ Project Charter   ☐ Design Deliverables affected

☐ Project Scope   ☐ Requirement Deliverables ☐ Construction Deliverables affected

Impact Description – Describe the impact for each of the items checked. List all deliverables affected by change request

Alternatives – If applicable - provide up to three alternatives that could be implemented instead of the proposed change.

"Let's Grow North West Together"

DECADE OF ACTION FOR
ROAD SAFETY
2021 - 2030

ARRIVE ALIVE

ICT Steering Committee Recommendations

Review Date	Team Members	Notes	Recommendation
		2	☐ Evaluated ☐ Recommended ☐ Not Recommended ☐ Defer Until: [DATE]
			☐ Recommended ☐ Not Recommended ☐ Defer Until: [DATE]

Rationale for Recommendation – State the rationale for the recommendation.

Change Request Management Approval (Head of Department)

Final Approval Date	Name	Title	Recommendation
			☐ Approve ☐ Reject

Special Instructions – Provide any additional information regarding the final recommendation.

Alternative Selected and Implemented – Provide a brief description of the alternative selected