Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

ICT CHANGE MANAGEMENT POLICY

Policy Registration 2026-03

TABLE OF CONTENTS

TERMS AND DEFINITIONS

Terms	Definitions
Change	Any transition or substitution within the environment.
Change Management Log	A category and detail list of all the requested changes in the ICT environment.
End-User	An official or authorised individual who utilises the information, computer equipment, and systems of the Department to perform their duties.
Executive Management	The highest level of leadership (e.g., CEO, CFO, COO) responsible for defining organisational strategy, setting long-term goals, and making high-stakes institutional decisions.
Head of Department	The Accounting Officer of the Eastern Cape Department of Social Development, as defined by the Public Finance Management Act.
ICT Change Management Board	A committee appointed by the Accounting Officer to deal with all the change requests in the ICT environment from system owners.
Members of Executive the Councillor	The Executive Authority appointed by the Premier to provide political leadership and oversight to the Provincial Department.
Acronyms	
AGSA	Auditor General South Africa
CGICTPF	Corporate Governance of ICT Policy framework
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
DPSA	Department of Public Service Administration
DRP	Disaster Recovery Plan
ECDSD	Eastern Cape Department of Social Development
GITO	Government Information Technology Officer
HOD	Head of Department
ICT	Information and Communication Technology
IT	Information Technology
ITIL	Information Technology Information Library
ISF	Information Security Forum
ISO/IEC	International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC)
MISS	Minimum Information Security Standard
SLA	Service Level Agreement

LEGISLATIVE FRAMEWORKS

1. Constitution of the Republic of South Africa,1996
2. Public Finance Management Act (Act No. 1 of 1999)
3. The Promotion of Access to Information Act (Act No. 2 of 2000)
4. Promotion of Administrative Justice Act (Act No. 3 of 2000)
5. Protection of Personal Information Act (Act No. 4 of 2013)
6. Labour Relations Act (Act No.12 of 2002)
7. Control of Access to Public Premises Act (Act No. 53 of 1985)
8. Minimum Information Security Standard (1996)
9. Occupational Health and Safety Act (Act No. 85 of 1993)
10. State Information Technology Act (Act No. 88 of 1998)
11. White Paper on the Transformation of Public Service, 1995
12. Treasury Regulations 17 of 2005
13. Change Management Strategy Framework of 2013
14. National Development Plan 2030
15. Public Service Regulation, 2016

1. PREAMBLE

Since its implementation in 2020, this policy's core controls have remained relevant and effective. However, the rapid evolution of computer technology and network systems has introduced sophisticated threats to information security. Protecting the department's information assets now requires more robust management standards and control measures to mitigate escalating security risks.

This policy mandates the execution of ICT technical changes in strict alignment with current legislation and the **Minimum Information Security Standards (MISS)** as issued by National Intelligence.

The Change Management Policy serves as the definitive statement of management intent regarding the ICT environment. It ensures that every modification follows a standardised, authorised process designed to protect the availability, confidentiality, and integrity of all systems and assets.

2. PURPOSE

The purpose of this policy is to provide for the implementation of ICT change management strategies to mitigate information corruption, ICT production performance issues, productivity losses and exposure to reputational risk.

3. OBJECTIVES

a) To establish management direction and high-level objectives for ICT change management.
b) To ensure that changes proposed are documented, reviewed, authorised, tested, implemented, and released in a controlled manner.

4. SCOPE OF APPLICABILITY

This policy is applicable to all employees, contract workers and individuals granted access to departmental systems.

5. PRINCIPLES AND VALUES

a) **Confidentiality:** The departmental employees shall be ethical and maintain the legal obligation to protect sensitive information.
b) **Integrity:** Employees shall practise honesty, consistency and be ethically firm.
c) **Availability:** The Department shall ensure systems and resources remain accessible.
d) **Accountability:** The Department shall ensure employees take responsibility for actions and outcomes.

6. POLICY PROVISIONS

6.1 General Requirements

The Head of ICT shall ensure that:

a) Controls for ICT operations are documented including employee duties and formal methods to implement changes to ICT systems and information assets.
b) A formal change control procedure is documented and enforced to govern the application of computer installation, Data Centre SAN or servers, networks, and system development changes to production environment.
c) The relevant system owner approves all business application changes with a financial impact.
d) The Head of ICT/GITO or delegated senior official recommend all infrastructure/architectural changes.

6.2. Change Management Procedures

Change to the department information resource and information asset such as, operating systems, computing hardware, networks, and applications shall be performed according to these Change Management Procedures:

a) Ensuring proposed changes are reviewed for relevance and impact.
b) Ensuring change management procedure is formally defined, documented, and adhered to.
c) Ensuring changes affecting computing environmental facilities are reported and coordinated with ICT Management.
d) Ensuring the Change Management Board/ICT Operations Committee are approved by HOD in terms of CGICTPF.
e) Ensuring a formal written change request is submitted for changes, both scheduled and unscheduled.
f) Ensuring scheduled change request are submitted in accordance with change management procedures.
g) Ensuring scheduled change requests receive formal Change Management Board/ICT operations committee approval.
h) Ensuring the appointed chairperson of the Change Management Board/ICT Operations Committee is able to deny a scheduled or unscheduled change.
i) Ensuring changes are fully tested in an isolated, controlled, and representative environment.
j) Ensuring software change or update is controlled with version control.
k) Ensuring usage of live data for testing new systems and systems changes.
l) Ensuring data is protected against unauthorised or accidental changes.
m) Ensuring fallback procedures for aborting and recovering unsuccessful changes are documented and tested.
n) Ensuring emergency changes are authorised and recorded.
o) Ensuring disaster recovery plans are updated with relevant changes, managed through change control process.

p) Ensuring information resources documentations are updated when each change is complete and old documentation are archived or disposed.

q) Ensuring customer notifications are completed for each scheduled or unscheduled.

r) Ensuring change review are completed for each change, scheduled or unscheduled.

6.3. Change Management Log

The change management logs shall be maintained for changes. The log shall contain:

a) Date of submission and date of change.

b) Owner and custodian contact information.

c) Nature of the change.

d) Indication of success or failure.

6.4. Data Testing

Data for test and research purposes shall be de-personalised prior to release to testers unless everyone involved in the testing has authorised access to the data.

6.5. Changes or modifications

Changes or modifications to MIS systems, networks, programmes, or data shall be approved by the system owner.

6.6. Fall-back Procedures

a) The Department shall ensure fallback procedures for aborting and recovering unsuccessful changes are documented and tested.

b) 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.

c) Fall back procedures shall be in place to ensure systems can revert to what they were prior to implementation of changes.

d) A back up shall be taken before any deployment or configuration status should be readily available for reconfiguration if there is need.

7. APPROVING AUTHORITY

The Member of the Executive Council and the Head of Department have the responsibility to approve this policy.

7. EXCEPTIONS/EXEMPTIONS

There are generally no exceptions or exemptions to the provisions of this policy, and any situation-based exceptions shall be approved by the Head of Department in line with established protocols to come into effect.

9. ADMINISTRATION OF THE POLICY

The administration of this policy shall be vested on the Head of Department to ensure employees adhere to the provisions of this policy.

10 ACCOUNTABILITIES AND RESPONSIBILITIES

10.1. ICT Governance Structures

The ICT Governance structures shall be responsible for ensuring implementation compliance, maintenance of this policy and generally advising on information security controls improvements.

10.2. Information Systems Owners

a) Shall be responsible for analysing and forming part of the authorisation list, recommending, and approving all changes that affect the business system.
b) Shall be responsible for alignment of the business system with business strategy, legislation, and policies.

10.3. All Employees

a) All employees shall be responsible for complying with this policy.
b) Users of the business system shall propose changes to the system or identify areas of improvements and refer to ICT for attention.
c) Third party employees shall comply with information security policies.

10.4. Member of the Executive Council

The member of the Executive Council shall be responsible for the approval of this policy.

10.5. The Head of Department

The Head of Department working in conjunction with the CIO shall be responsible for ensuring the effective implementation and compliance of these policies and standards procedures.

11. EFFECTIVE DATE OF THE POLICY

This policy shall be implemented from its effective date approval.

12. MONITORING MECHANISMS

The CIO and senior management shall be required to ensure ICT Operational Committee, ICT Steering Committee and the Risk Committee exist to monitor and measure compliance with this policy.

13. ENFORCEMENT

Non-adherence with the provisions of this policy shall result in disciplinary proceedings.

14. POLICY REVIEW

This policy shall be reviewed after three years (3) and whenever there are new developments or legislation change.

15. POLICY RECOMMENDATIONS AND APPROVAL

Recommended/Not Recommended

MR. M. MACHEMBA
HEAD OF DEPARTMNET
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 04/05/2026

Approved/Not Approved

MS. B. FANTA
MEMBER OF THE EXECUTIVE COUNCIL
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 04/05/2026