Province of the
EASTERN CAPE
OFFICE OF THE PREMIER

Provincial
ICT Change Management
Policy

LEADING DEVELOPMENT WITH EXCELLENCE AND INTEGRITY

Notice

DOCUMENT DETAILS

I. Document Title

Version	1.1
Issue Date	30 August 2022
Document Name	Provincial ICT Change Management Policy
Prepared by	Provincial ICT-Office of the Premier
Document Enquiries	The primary contact for enquiries regarding this document is:
Name	Siphokazi Ngqungqu
Organization	Eastern Cape Office of the Premier – Provincial ICT
Title	Director: Systems Development
Phone	082 798 3440
e-mail	Siphokazi.Ngqungqu@ecotp.gov.za

II. Version Control

Version #	Date	Reason for Change	Author
0.1	October 2021	1st draft	Zimasa Mqamelo
0.2	22 February 2022	Provincial ICT & PGITOC Input	Siphokazi Ngqungqu
0.3	31 May 2022	Input from ICT Steering Committee	Siphokazi Ngqungqu
0.4	22 August 2022	Recommendations from Shared Legal Services	Siphokazi Ngqungqu

III. Approvals

The contents of this version of the document are accepted and approved without any alteration by the following signatories.

On Behalf of the Eastern Cape Provincial Government ***Director General (DG) of OTP*** *Mr. M. Sogoni*	
	04 November 2022
Signature	***Date***

IV. Acronyms

No	Term	Definition
1.	OTP	Office of the Premier
2.	EC	Eastern Cape
3.	ECOTP	Eastern Cape Office of the Premier
4.	ICT	Information and Communication Technology
5.	CCB	Change Control Board
6.	ECCB	Emergency Change Control Board
7.	CIO	Chief Information Officer
8.	PGITOC	Provincial Government Information Technology Council
9.	CI/s	Configuration Item/s
10.	PSA	Public Service Act
11.	DPSA	Department of Public Service and Administration
12.	PSR	Public Service Regulation

V. Definition of Terms & Concepts

No	Term	Definition
1.	Departments	All 13 Eastern Cape Provincial Departments
2.	Change	Refers to any addition, deletion modification or replacement or any combination of the afore going of an ICT resource.
3.	ICT Change Control Board	A dynamically formed group of functional experts, who assist in assessing, prioritizing, scheduling, and authorizing changes.
4.	Change Manager	Refer to the official that oversees the implementation of change management process.
5.	Release	Refer a collective of hardware, software, documentation, process, or other components required to implement one or more approved changes to ICT Services.
6.	Service provider	Refers to third party that is responsible for the supply of services and/or goods for delivery of ICT service.
7.	Change Owner/Requestor	This person initiates a Request for Change (RFC) and may reside within the operational unit in a department.
8.	End-user Department	Refers to the end-user department responsible for executing the business process that has been automated or is utilizing the system where the change is required.
9.	Change Authorizer	Refers to HOD or delegated official responsible for approving change request in the department.
10.	Configuration Item	Refers to any service component that needs to be managed to ensure successful delivery of service.
11.	Provincial ICT	Refers to the Chief Directorate based in OTP and is responsible for providing ICT support to departments specifically for Transversal Systems and Infrastructure.
12.	Incident	Refer to an unplanned interruption to an IT service or reduction in the quality of an IT service.
13.	ICT resource	Refers to any institution’s asset related to ICT. It may include tangible (e.g. hardware) and intangible (e.g. software) resources.

14.	Change Implementer	Refers to the official responsible for the ongoing administration of technologies such as servers, databases and network devices that are within the scope of the ICT change management process.
15.	Change Coordinator	Refers to the official responsible for assisting in Request for Change (RFC) documentation review for an IT group, department, or division. This role is fulfilled by a Functional Support Analyst/ Business Analyst/or a delegated official.
16.	CCB Member	Refers to the official responsible for attending scheduled meetings or sends a representative and is empowered to make decisions on behalf of the operational area he or she represents.
17.	Major Change	Refer to change that potentially affect more than one department or the entire provincial government.
18.	Significant Change	refer to a change that may affect few end-users and but multiple ICT components in multiple departments.
19.	Emergency change	Refers to an urgent, mandatory change that may occur outside the scheduled downtime where critical changes impacting on ICT service must be performed to restore service availability.
20.	Standard Change	Refers to a pre-authorized change that follow a well-known standardized procedure.
21.	Service Transition	Refers the coordinated manner of introducing changes to ICT environment.
22.	ICT Architecture	Refers to a specifications, models, and design of information asset of an institution including hardware, software, and infrastructure.

Contents

1. Policy Background

The ICT Change Management Policy has been in use since 2013. The 2013 version is however now due for review. The review has established that the objectives of the control are still relevant in their current form. The area that needed strengthening is the area of change review/impact assessment and an establishment of Change Control Board.

2. Purpose

The purpose of this ICT Change Management Policy is to control changes in the ICT (Information & Communications Technology) environment. It is also to set out a defined process to be followed when changes are required in ICT services.

3. Policy Aims and Objectives

The objectives of the Change Management process are to:

a) Ensure that standardized methods and procedures are used for the efficient and prompt handling of all changes, to minimize the negative impact of changes upon service quality, and day-to-day operations.

b) Ensure only authorized changes are made to the ICT production environment.

c) Respond to the Departments' ICT changing business requirements while maximizing value and reducing incidents and disruptions.

d) Ensure ICT provide services that respond appropriately to department operational needs.

e) Ensure that a consistent approach is used in managing changes.

4. Consultation Process

The policy was circulated to employees in Provincial ICT and Departmental ICT in the Office of the Premier and the Provincial Government Information Technology Officer Council (PGITOC) for input. The input has been considered in the development of this document.

5. Regulatory Framework

This policy has been developed in terms of the following prescripts

i. **Section 3(1) of the Public Service Act (PSA) of 1994**, as amended, mandates the Minister for Public Service and Administration to establish norms and standards that inform proper management and functioning of national and provincial departments. These norms and standards referred to in Section 3(1) include inter alia matters relating to the optimal utilization of IT as a valuable and scarce resource.

ii. **Chapter 6 of the Public Service Regulation (PSR) of 2016: Information management and electronic government (regulations 93)** indicates that the head of department shall ensure that the acquisition, management, and use of information technology by the department improve-

   (a) direct or indirect service delivery to the public, including, but not limited to, equal access by the public to services delivered by the department.

   (b) the productivity of the department; and

   (c) the cost-efficiency of the department.

iii. **Department of Public Service and Administration (DPSA) ICT Security Guideline of 2017 Section 11.7 that** deals with Information Systems Acquisitions, Development and Maintenance paragraph 3 indicates that when operating platforms are developed or changed, applications should be reviewed and tested to ensure there is no adverse impact on the institution’s operations.

iv. **DPSA ICT Security Guideline of 2017 Section 11.7** that deals with Information Systems Acquisitions, Development and Maintenance, paragraph 5 indicates that changes to ICT systems should be controlled through formal change control procedures from the design throughout to the maintenance phase.

v. **DPSA, Implementation Guideline for Corporate Governance ICT Policy Framework, 2014** indicates that an institution must provide relevant ICT resources, organizational structure, capacity, and capability to enable ICT service deliver.

6. Scope and Applicability

This policy covers the management of ICT changes due to the release of any new services or a service change to the Departments’ ICT architecture.

a) Changes include additions, deletions, and modifications to any ICT Architecture resource.

b) The Departments’ ICT architecture includes, but is not limited to, hardware, software, operating systems, data and voice network, and applications.

This policy should be read in conjunction with Terms of Reference for ICT Change Control Board and change management procedure.

7. Policy Statements

a) ICT service and infrastructure changes shall have a clearly defined and documented scope.

b) All changes shall be recorded and classified according to type i.e. standard, normal, and emergency.

c) A change shall be categorized as major or significant depending on the number of end-users that will be affected by it.

d) Requests for all changes shall be assessed for their risks, impact, and operational benefit.

e) The change management process shall include how the change shall be reversed or remedied if unsuccessful.

f) All changes shall be authorized by a duly authorized person or delegated official and shall be implemented in a controlled manner.

g) The end-user must be kept updated on the status of changes as and when required.

h) All emergency changes shall be implemented as outlined in the ICT change management procedure and a report sent to the CCB.

i) All normal changes shall be implemented as per change and release schedule.

j) A schedule of all the changes approved for implementation and their proposed implementation dates shall be maintained and communicated to relevant parties.

k) There shall be appropriate segregation of duties in authorization and implementation of all changes.

l) ICT Change Control Board meetings shall be held on a quarterly basis.

m) Emergency changes will be implemented as outlined in the ICT change management procedure.

n) Once the changes have been implemented the ICT disaster recovery plans should be updated accordingly.

o) End-user must be notified of the status of change throughout the change management process.

p) A post implementation review must be completed for each change implemented.

8. Role and Responsibilities

Responsibilities for implementing this policy are set out below:

a) All ICT staff and end-users of the provincial Departments have the responsibility in the implementation of the Change Management process:

   i. **End-User-** has the responsibility for submitting an approved change request to ICT, and to participate in the testing of that change where applicable.

   ii. **Change Owner / Head of the Operational End user Unit** has the responsibility for ensuring that the change process is followed for all system changes and all required approvals are adhered to.

   iii. **Change Authorizer** has the responsibility to approve request for change. This role will be the responsibility of the Head of Department or delegated official of that respective department that requested the change.

   iv. **Provincial ICT** – has the responsibility of following the prescribed change management process and procedures and that the policy relevancy is maintained.

   v. **Change Control Board (CCB)** – has the responsibility is to assess, prioritize, recommend authorization of all ICT change requests.

   vi. **Change Control Board member**– has the responsibility to participate in review of the change requests and make input on CCB recommendations.

   vii. **Emergency Change Control Board** – has the responsibility is to assess, prioritize, authorize, and schedule emergency ICT change requests. It also needs to submit a report of all emergency changes implemented to the CCB.

   viii. **Change Manager -Director Systems/ Infrastructure**– has the responsibility for overseeing approval of changes to the ICT architecture.

   ix. **Change Coordinator**: responsible for coordinating all role players during the change management process.

   x. **Chief Information Officer (CIO)** – has overall governance responsibility for overseeing the change management policy and processes. This includes, but is not limited to, policy dissemination, process enforcement and chairing the ICT Change Control Board.

b) All service providers responsible for providing services to the Departments' ICT Architecture must comply with this policy.

   i. Service providers of externally hosted services are responsible and accountable for informing the Departments of their role and responsibilities in its change management process.

   ii. For hybrid services (contains service components owned/managed by the Departments) the departments and service providers will work collaboratively during service transition (moving ICT changes from development to operations) to ensure compliance.

9. Policy Monitoring and Evaluation

The following governance structures will monitor the implementation of this policy.

a) ICT Operational Committee

b) ICT Steering Committee

c) PGITO Council

d) ICT Change Control Board

The CIO and senior management in the respective Departments are required to ensure that internal audit mechanisms exist to monitor compliance with this policy. The Internal Audit department is authorised by management to assess compliance with all policies at any time.

10. Effective Date

The policy will be effective from the date the Director General approves it.

11. Policy Review

The policy will be reviewed in line with Medium Term Strategic Framework or whenever there are new developments to maintain relevance.

12. References

I. Department of Public Service & Administration, Public Service Act, 2001

II. Department of Public Service & Administration, Public Service Regulations, 2016

III. Department of Public Service & Administration, Information Security Guidelines, 2017

IV. Department of Public Service & Administration, implementation Guide for Corporate Governance of ICT Policy Framework, 2014

V. Axelos, ITIL Foundation Handbook, 2012, TSO Publishers