LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
CO-OPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

REVIEWED ICT CHANGE MANAGEMENT POLICY

Version: 2

Table of Contents

I. Acronyms and Abbreviations

CAB	Change Advisory Board
CoGHSTA	Cooperative Governance, Human Settlement and Traditional Affairs
GITO	Government Information Technology Office(r)
ICT	Information Communication Technology
SLA	Service Level Agreement
VPN	Virtual Private Network

II. Clarification of Terms

Accountability: ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action.

Authentication: establishing the validity of a claimed entity/verification of the identity of an individual or application.

Availability: being accessible and useable upon demand by an authorized entity.

Confidentiality: the principle that information is not made available or disclosed to unauthorized individuals, entities or processes.

Information and communication systems: applications and systems to support the business, utilizing information technology as an enabler or tool.

Information technology: any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information.

Monitoring: performance measurement to ensure the confidentiality, availability and integrity of operational systems and information.

1. Preamble

1.1. The complexity of current business environments, and the diverse technology used in ICT infrastructure environments demands a greater control to minimize risk and potential impact on the business.

1.2. Procedures should be instituted to ensure all ICT changes are recorded, followed up and escalated to management when necessary. It is important that these procedures are adhered to at all times.

2. Purpose and objectives

2.1. The purpose of this policy is to provide the COGHSTA with a procedure for the ICT change control function that shall be established to manage record and track all changes for CoGHSTA ICT environment.

2.2. The objective of this policy is to ensure that standardized processes are followed and adhered to accordingly. This is to ensure that no ICT changes take place as a quick change, with documentation provided afterwards, without any prior authorisation.

3. Scope of Application

This policy is applicable to all employees of the COGHSTA, including learners and interns as well as all other stakeholders who make use of the COGHSTA ICT network and systems.

4. Legal Framework

The following publications govern the execution of the Internet Use Policy and were taken into consideration during the drafting of the Policy:

4.1. State Information Technology Act (Act no 88 of 1998)

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

4.3. Minimum Information Security Standards (MISS), Second Edition March 1998

4.4. Departmental Email Policy

4.5. Departmental Internet Usage Policy

4.6. Departmental Password Policy

4.7. Departmental ICT Security Policy

4.8. Departmental ICT Equipment Usage Policy.

5. Administration of the policy

GITO is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

6. Policy Content

The ICT Change Management Process seeks to manage and control the ICT changes through processes and procedures and then ensuring that the appropriate authority levels exist for each ICT change.

The following process steps shall be used within CoGHSTA:

6.1. Change Initiation

6.1.2. An ICT change is initiated when the requirements for a change has been identified. This request for change can be initiated for the following reasons:

(a) Change to infrastructure components.

(b) Resolving problems.

(c) Project related activities.

(d) Ad-hoc activities that influence service delivery.

6.2. Change Planning and Building

6.2.1. Under the responsibility of change planning and building, ICT changes may be scheduled and planning may be provided if necessary for the optimum control of the change.

6.2.2. ICT Change Management has a coordination role, supported by line management, to ensure that activities are both resourced and also completed according to schedule.

6.3. Change Logging and Filtering

6.3.1. Under the responsibility of the ICT Help Desk, changes are logged on the Help Desk Remedy system.

6.3.2. Each ICT Change may be categorized accordingly in the automatic function of the Help Desk Remedy system.

6.3.3. A Request for ICT Change Form (Annexure A) needs to be completed for the following changes to the ICT environment:

CLASS	ITEM	DEFINITION
Significant	Install	New requirement introduced
Minor	Move	Move of any component within the Infrastructure environment
Significant	Addition	Additional requirements (including releases and or upgrades) within the Infrastructure environment
Minor	Configuration	A change to the function or the assembly to the Infrastructure environment
Significant	Decommission	Removal of any component from the

		Infrastructure environment
Minor	Operational state	Change from the current operation state of a component within the Infrastructure environment

6.3.4. There are two change types that needs to be adhered to base on the above classes and items:

CHANGE TYPE	**DEFINITION**
CAB Changes	For changes that need to be channeled via the CAB after which approval or rejection will be provided
Pre-approved changes	For changes that can take place without being channeled via the CAB, e.g. password resets / creation of new user accounts
CAB CHANGES	**PRE-APPROVED CHANGES**
May cause down-time on production systems	May not cause down-time on any system
May affect one or more SLAs	May not affect any SLA
May affect configuration information	May not affect any processes
May affect processes for services	
Changed with high risk involved	

6.4. Emergency Changes

The emergency ICT change management process shall provide a change control mechanism in the event of an emergency. The goal is not to bypass the ICT Change Management Processes but rather to speed up the process and execute it quickly and efficiently when the normal process cannot be followed due to an emergency.

The following criteria shall be accepted as Emergency Changes

(a) Production loss

(b) Financial loss

(c) Prevention of death

(d)Legislation changes

6.5. ICT Change Approval

6.5.1. Prior to the approval of ICT changes, an approval indicator shall be allocated to the change to enable the correct workflow associated with the required approval. The risks of the ICT Change will determine the required approval:

CATEGORY	VALUES		
	1	2	3
1. Change Classification	Major	Significant	Minor
2. Priority	High	Medium	Low
3. Impact	Multiple districts	Single district	No impact
4. Implementation	Exceed 4 hours	Complex	Simple
5. Black out	Exceed 4 hours	Complex	Simple

6.5.2. The sum of the value of the five risk categories may determine the approval process:

Low risk	**Greater than 10 = Minor Approval required**
Medium risk	**From 6 to 10 = Significant Approval required**
High risk	**Less than 6 = Major Approval required**

6.5.3. The risk factor indicates the nature of the approval:

Minor Approval	The Chairperson of the CAB has delegated authority to approve and schedule changes to the Senior Manager: Information Technology and shall report back to CAB
Significant Approval	The change submitted shall be discussed at the CAB and relevant documentation are sent to CAB members before the meeting for assessment
Major Approval	GITO shall raise the Request for Change with the CAB. Approved changes must be passed back to the CAB for scheduling and implementation
Emergency Approval	Request for Change forms and relevant documentation are sent to CAB members for approval. A minimum of two members need to approve the change

6.6. ICT Change Implementation

6.6.1. GITO shall be responsible for implementation of all ICT changes as scheduled.

6.6.2. Feedback regarding the success or failure of the ICT change shall be provided to the CAB within 5 days after the planned completion time.

6.7. ICT Change Review and Reporting

6.7.1. GITO management shall perform an evaluation of the ICT changes implemented. The purpose of this review shall be:

6.7.2. Establish if the change had the desire effect and met the objectives;

6.7.3. Tasks and follow-up actions assigned to correct any problems or inefficiencies arising in the change management process itself as a result of ineffective changes;

6.7.4. Where resources were used to implement the change as planned, and any problems or discrepancies fed back to CAB helping to improve the future estimating process; and

6.7.5. Review satisfactory and abandoned changes, and formally closes them in the ICT help desk system.

6.8. Communication

Communication will be managed according to the predefined communication structure for each project. Communication shall include:

a) Change approvals
b) Change notifications
c) Change control escalations
d) Change management processes and procedure changes
e) Change management standard changes
f) Change management policy changes.

7. Roles and responsibilities

Different owners of processes and responsibilities can be identified.

7.1. Owner: Change Management

The Senior Manager within GITO shall be responsible for:

7.1.1. Defining of the ICT Change Management process, procedure, division of work and the roles and responsibilities within the process

7.1.2. Contributing to the evaluation or establishment of the ICT change management system, ensuring conformance to documentation standards

7.1.3. Maintaining the ICT change management system in accordance with agreed procedures

7.1.4. Reviews on procedures and other processes checking for compliance against the quality system, and external standards where appropriate

7.1.5. Communicating all updates and/or changes of the ICT Change Management Process

7.1.6. Promoting awareness of the importance of a structured ICT change management process, working with other business units

7.2. ICT Change Advisory Board

7.2.1. The Department shall formulate an ICT Change Advisory Board to function within the following mandate:

7.2.1.1. To formalize an official forum to review all ICT changes in a structured way.

7.2.1.2. To focus the attention of the Committee to the management of ICT changes.

7.2.2. The ICT Change Advisory Board shall:

7.2.2.1. Review all high impact ICT changes to be implemented.

7.2.2.2. Review any ICT change that was implemented unsuccessfully or had to be cancelled.

7.2.2.3. Screen all the ICT changes to ensure the correct category, type and item have been selected.

7.2.2.4. Monitor routine and low impact ICT changes.

7.3. GITO

7.3.1. Implement Change requests as per above mentioned ICT Change Management Process.

7.3.2. Provide regular feedback on progress regarding the change request and schedule.

8. Change Lead

8.1. Change lead time is the amount of time required to evaluate and adequately plan for change implementation. Lead time is measured from the time the change is submitted until the change is actually implemented. Lead time shall vary by the type of change.

8.2. All changes to be submitted shall be done within the following lead time matrix:

SERVICE	LEAD TIME
APPLICATION SYSTEMS	
New Application Releases	1 month
Incident Fixes	12 – 24 hours
Emergencies	12 hours
OPERATIONS	
Installation of hardware	1 – 2 months
Consumable – tapes / cartridges	2 weeks
Changes to Schedules	48 hours
Hardware maintenance	1 month
Changes to operation of servers	1 week
NETWORK	
Installation of new data lines	4 months
In- and outdoor transfer of data lines	1 month
Installation of new equipment on existing network	2 weeks
Incident fixes	3 weeks
TECHNICAL SUPPORT	
New application release	3 weeks
Environmental changes	2 months

Incident fixes	24 – 48 hours
Software evaluation	2 weeks
The lead time for non-standard changes that require research shall be negotiated with SBU's concerned, and will depend on the nature and complexity of the change or captured in Operational Service Level Agreements	

9. Default

Non-compliance of this policy shall constitute violation of the policy and shall be treated in terms of the departmental disciplinary code and procedure policy.

10. Inception Date

This policy comes into effect from the date of approval by Member of Executive Council.

11. Policy Review

This policy shall be reviewed bi-annually.

12. Enquiries

Enquiries about the policy should be directed to the Government Information Technology Office.

Document Title	**ICT Change Management Policy**
Compiled by :	**Government Information Technology Office** **Senior Manager** **(ICT Infrastructure and Systems)** **Date** 24/12/2014
Acknowledge by :	 **General Manager (GITO)** Acting **Date** 24/12/2014
Qualified by:	 **Senior Manager** **(Research and Policy Coordination)** **Date** 24/12/2014
Recommended by:	 **Senior General Manager** **(Corporate Services)** **Date** 05th/01/2015
Adopted by :	 **Head of Department** **Date** 07/01/2015
Approved by :	 **Member of the Executive Council** **Date** 07/01/2015

ANNEXURE A

LIMPOPO PROVINCIAL GOVERNMENT REPUBLIC OF SOUTH AFRICA DEPARTMENT OF COOPERATIVE GOVERNANCE, HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS	**ICT INFRASTRUCTURE**	Logged By:	
		Card Number:	
		015-284-5591	

REQUEST FOR CHANGE

Requestor Details

Full Name		Persal No:	
Business Unit:			
Telephone:		Building:	
Cell Number:		Floor:	
Town:		Office No:	

Details of the Change Request

Date		
Describe the change that is being requested, including systems and components:		
Outline your motivation for this in terms of impacts, risks and benefits.		
Additional information:		

Signatures

DECLARATION BY EMPLOYEE: By signing this form I confirm that the change is required for operational business purpose.

Role	***Position***	***Name***	***Signature***	***Date***
Requester				
Approved by:				
Implemented by:				
Verified by:				