CAPRICORN DISTRICT MUNICIPALITY

EXTRACT FROM THE MINUTES OF COUNCIL MEETING HELD ON 29 JUNE 2017

ITEM

SC 13/2016-2017/5.1.5 **Reviewed Information and Communication Technology (ICT) Policies**

RESOLUTION

Resolved, That the following reviewed Information and Communication Technology (ICT) Policies be approved:

(a) Backup Policy;
(b) Data Centre Access Control and Environmental Policy;
(c) Change Management Policy;
(d) Notebook and Tablet Policy;
(e) Password Policy;
(f) ICT Account Management Policy;
(g) Electronic Mail Policy;
(h) Internet Policy;
(i) IT Security Acceptable Use Policy; and
(j) Municipal Corporate Governance of Information and Communication Technology Policy.

CERTIFIED AS A TRUE EXTRACT FROM THE MINUTES.

NM LEKGANYANE
COUNCIL SPEAKER

2017/06/29
DATE

CAPRICORN DISTRICT MUNICIPALITY
OFFICE OF THE SPEAKER
2017 -06- 29
LIMPOPO PROVINCE

CAPRICORN

DISTRICT MUNICIPALITY

SUBMISSION

Date: 26 JUNE 2017 **Memo Ref: 5/1/4**

TO : COUNCIL
DATE : 29 JUNE 2017
FROM : MAYORAL COMMITTEE
SUBJECT : INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICIES

1. PURPOSE

The purpose of the submission is to request Council to approve the review of Information and Communications Technology (ICT) policies.

2. BACKGROUND

The Municipality utilises data on a daily basis to perform its duties. This data needs to be effectively managed and secured to ensure that it is available as and when required. ICT and IKM unit has therefore implemented Policies to manage data, systems and access and to ensure effective use of ICT.

Some of these Policies were approved by Council and are now in the process of being reviewed.

The objectives of the policies are as follows:

Name of Policy	**Policy Objective**
ICT Backup Policy	The policy is aimed manage backup of data utilised by the Municipality. The policy outlines what data has to be backed up, how to store data and how to restore data
ICT Data Centre Access Control Policy	To manage access of the Server room and to ensure that physical conditioned of the server room is protected against fire and any other disaster.
ICT Change management Policy	To manage all changes done on all ICT systems. Changes are categorised in major

	and minor and relevant approval is required for every change.
ICT Notebook Policy	To manage the allocation, protection and the use of Municipal Laptops/Tablets
ICT Password Policy	To manage the use of passwords and password credentials, reset and unlock password.
ICT Account Management Policy	To manage the creation, modification and termination of user on the system
ICT Email Policy	To manage the use of email, the size of email and the language to be used when communicating through email.
ICT Internet Policy	To manage the use and access of Internet. It also list prohibited sites and restricted downloads
ICT Security Policy	To manage security and ensure that data is secured. It also outlines all security measures on the systems, infrastructure and network.
Municipal ICT Governance policy	To regulate Governance of ICT within the Municipality to ensure that ICT support Municipal strategies and that Municipal Council, Executive Management and Management plays a role in ICT initiative.

3. INPUTS FROM RELEVANT STRUCTURES

3.1 Inputs from Corporate Services Portfolio Committee

To include a table of policy number, date of approval, date of review by each committee on each policy so that the Municipality is able to easily track dates

3.2 Inputs from LLF Sub Committee (Basic Condition)

3.2.1 All Policies should be reviewed as and when required and not every two years.

3.2.2 Tablets for Councillors should be revised as follows:

- Provision of tools of trade for Councillors will be done in line with rules and regulations as determined by the upper limits and applicable legislation
- Wi-Fi access should be included in the policy.

4. RECOMMENDATION

That Council approves the reviewed Information and Communications Technology (ICT) policies.

CLLR M.J. MPE
EXECUTIVE MAYOR

2017/06/26
DATE

CAPRICORN
DISTRICT MUNICIPALITY

ICT
CHANGE MANAGEMENT POLICY
Policy ref number: 10/5/P-9

DOCUMENT VERSION CONTROL			
Version	Version Date	Nature of Change	Changed by Person
1.0	07 August 2015	New Document	Corporate Services Department
1.1	25 August 2015	Review and Update	Executive Management
1.2	14 December 2015 09 May 2016	Review and Update	Management
1.3	29 March 2017	Review and Update	LLF Subcommitee
1.4	08 June 2017	Review and Update	LLF
1.5	19 June 2017	Review and Update	Corporate Services portfolio
1.6	26 June 2017	Review and Update	Mayoral
1.7			Council

TABLE OF CONTENT

1. PREAMBLE

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.

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

2. TERMS AND DEFINITIONS

2.1 Accountability means ensuring that the actions of an entity or individual may be traced uniquely to that entity or individual, who may then be held responsible for that action;

2.2 Authentication means establishing the validity of a claimed entity/verification of the identity of an individual or application;

2.3 Availability means being accessible and useable upon demand by an authorised entity;

2.4 CAB means Departmental Change Advisory Board.

2.5 Confidentiality means the principle that information is not made available or disclosed to unauthorized individuals, entities or processes;

2.6 Monitoring means performance measurement to ensure the confidentiality, availability and integrity of operational systems and information;

2.7 VPN means Virtual Private Network;

2.8 SLA means Service Level Agreement;

3. ACRONYMS AND ABBREVIATIONS

CDM - Capricorn District Municipality

ICT - Information and Communications Technology

ISO – Information Security Standards

MISS– Minimum information security standard

4. INTRODUCTION

The POLICY document the way that we manage changes that occur to CDM maintained information technology in a way that minimizes risk and impact to the municipality.

5. PURPOSE

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

6. POLICY OBJECTIVES

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

7. LEGISLATIVE FRAMEWORK

The following publications govern the execution of the ICT Change Management Policy and were taken into consideration during the drafting of the guidelines and policy:

(a) Protection of Information Act (Act no 84 of 1982);

(b) Minimum Information Security Standards (MISS), Second Edition March 1998;

8. SCOPE OF THE POLICY

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

9. POLICY PRINCIPLES

9.1 Consultation

All stakeholders who will be affected by the implementation of this policy will be consulted at all stages of the development or review of a policy

9.2 Information

All employee who are affected by a policy will be made aware of the policy

9.3 Batho pele priniples

Policies developed within CDM will consider all the Batho Pele Principles

10. PROCESS OVERVIEW

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

The following process steps shall be used within Capricorn District Municipality:

10.1 Change Initiation

10.1.1 A 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.

10.2 Change Planning and Building

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

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

10.3 Change Logging and Filtering

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

10.3.2 Each Change may be categorized accordingly in the automatic function of the Help Desk system.

10.3.3 A Request for 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

10.3.4 There are two change types that needs to be adhered to based on the above classes and items:

CHANGE TYPE	DEFINITION
Normal Changes	For changes that need to be channeled through 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

NORMAL 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	

10.4 Emergency Changes

10.4.1 The emergency change management process shall provide a change control mechanism in the event of an emergency. The goal is not to bypass the 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.

10.4.2 The following criteria shall be accepted as Emergency Changes

(a) Production loss

(b) Financial loss

(c) Prevention of death

(d) Legislation changes

7.4.3. Immediate change should be granted and approved by the ICT Manager.

7.4.4 All emergency changes should be reported to management with reasons for allocation of emergency changes.

10.5 Change Approval

10.5.1 Prior to the approval of changes, an approval indicator shall be allocated to the change to enable the correct workflow associated with the required approval. The risks of the 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

10.5.2 The risk factor indicates the nature of the approval:

For all change requests, change request forms should be filled by the users department, this request must be approved by the Departmental Manager and implemented by

Minor Approval	The Manager ICT has delegated authority to approve and schedule changes to the Manager: Information Technology and shall report back to IT Steering Committee
Significant Approval	The Executive Manager of each department approves the change for ICT to implement
Project related approval	Request for Change should be done by the project Manager approved by IT Manager for implementation. Changes that affects modular departments, the executive Manager is required to approve the changes.

10.6 Change Implementation

10.6.1 IT Department shall be responsible for the implementation of all changes as scheduled.

10.7 Change Review and Reporting

10.7.1 IT Department management shall perform an evaluation of the changes implemented. The purpose of this review shall be:

10.7.1.1 Establish if the change had the desire effect and met the objectives

10.7.1.2 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

10.7.2 Review satisfactory and abandoned changed, and formally closes them in the ICT help desk system.

10.8 Communication

10.8.1 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

11. ROLES AND RESPONSIBILITIES

Different owners of processes and responsibilities can be identified.

11.1 ICT Manager: Change Management

The manager for change management shall be responsible for:

11.1.1 Defining of the Change Management process, procedure, division of work and the roles and responsibilities within the process

11.1.2 Contributing to the evaluation or establishment of the change management system, ensuring conformance to documentation standards

11.1.3 Maintaining the change management system in accordance with agreed procedures

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

11.1.5 Communicating all updates and/or changes of the Change Management Process

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

11.2 ICT Steering Committee

11.2.1 The Department shall formulate an ICT Steering Committee to function within the following mandate:

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

11.2.1.2 To focus the attention of the Committee to the management of changes.

11.2.2 The ICT Steering Committee shall:

11.2.2.1 Review all high impact changes to be implemented

11.2.2.2 Review any change that was implemented unsuccessfully or had to be cancelled

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

11.2.2.4 Monitor routine and low impact changes.

11.3 ICT SECTION

11.3.1 Implement Change requests as per above mentioned Change Management Process

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

12 CHANGE LEAD TIMES

12.1 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.

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

SERVICE	LEAD TIME
APPLICATION SYSTEMS	
New Application Releases	2 month
Incident Fixes	12 – 24 hours
Emergencies	12 hours
OPERATIONS	
Installation of hardware	1 – 2 months
Consumable – tapes / cartridges	1 Month
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	3 months
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	

13 IMPLEMENTATION AND MONITORING

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

14 CONSEQUENCES OF NON-COMPLIANCE

Non-compliance of this policy will lead to disciplinary action, taken against an official.

15 DISPUTE RESOLUTION

Any dispute that may arise out of interpretation and/or application of a policy will be resolved through Municipalities grievance and or disciplinary resolution procedure and the CCMA rules respectively

16 POLICY REVIEW

This policy shall be reviewed as and when required.

17 ENQUIRIES

Enquiries with regard to any matter relating to this policy will be directed to:

Executive Manager

Department: Corporate Services

Tel No: 015 294 1064

18 APPROVAL

This policy was approved by council on the ....day of ....

Signed by ....in his/her capacity as .... On

behalf of council, on the ....of..............................