# 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**

N.M. Lekganya

**NM LEKGANYANE**
**COUNCIL SPEAKER**

2017/06/29
**DATE**

# 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

# PASSWORD POLICY
## Policy ref number: 10/5/P-5

| 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<br>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

## PREAMBLE

This document outlines the complexity requirements and proper management practices of passwords for all computer systems at Capricorn district Municipality.

## ACRONYMS AND ABBREVIATIONS

CDM - Capricorn District Municipality

ICT - Information and Communications Technology

ISO – Information Security Standards

MISS– Minimum information security standard

SAP – Systems Applications Product

ESS WEB – Emergency Services System Web based

## DEFINITIONS

**User:** Any person granted an ICT user account with the Department

**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

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

**Identification and authentication:** functions to establish and verify the validity of the claimed identity of a user

**Information and communication systems:** applications and systems to support the business, utilising 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

**Integrity:** the inherent quality of protection that maintains the accuracy of entities of an information and communication system and ensures that the entities are not altered or destroyed in an unauthorized manner

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

**Password:** confidential authentication information composed of a string of characters

**Remote access:** the access of remote users to corporate IT services by means of telephone lines or 3G data card through a gateway/computing that is performed at a location that is distant from a central site, over a network connection

**ICT network user account**: An authorised user account, provided to a user, to be used solely by that user, for the purpose of accessing services as granted to that user account

## 1. INTRODUCTION

Passwords are one of the primary mechanisms that protect potentially sensitive official information systems and other resources from unauthorized use. While passwords are not the most secured way of protecting information and information systems, constructing secure passwords and ensuring proper password management is essential. Poor password management and protection can allow both the dissemination of information to unauthorized access to CDM resources. Poorly chosen passwords can be easily compromised. Password compromise can lead to inappropriate disclosure and use of CDM resources or sensitive information.

## 2. PURPOSE

The purpose of this policy is to establish minimum rules, guidelines and standards for passwords creation and management used to logon to CDM information systems.

## 3. SCOPE

This policy applies to all user accounts provided by CDM and all CDM employees, contractors and service providers that logon to CDM information computers and network.

## 4. LEGISLATIVE REQUIREMENTS

4.1 ISO 17799
4.2 Information Security Forum (Code of good practice for Information Security)
4.3 Minimum Information Security Standards
4.4 Protection of Information Act
4.5 COBIT Audit Framework

## 5. POLICY PRINCIPLES

### 5.1 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

### 5.2 Information

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

### 5.3 Batho pele priniples

Policies developed within CDM will consider all the Batho Pele Principles

## 6. POLICY STATEMENT

All user accounts used to logon to CDM information systems shall be protected with strong passwords. Furthermore, passwords must be changed regularly to avoid unauthorized access to information and information systems. Passwords that are not managed properly are at risk of accidental disclosure overtime.

## 6.1 Requirements

6.1.1 Every user must have a unique username

6.1.2 User accounts for temporary staff, contractors and service providers will be set to automatically expire on the last day of the contract. Should the contract be renewed, the user will be required to re-apply for network access. ICT (**Information and Communications Technology**) Support personnel will only re-enable the user account after receiving the new user application.

6.1.3 Initial passwords must be uniquely created by a random password generator and must be communicated to the user in a secure manner. The user must automatically be forced by the computer system to change this initial password upon initial user logon

6.1.4 Passwords may not be blank

6.1.5 ICT Support personnel will only give initial passwords, unlock accounts or reset passwords once the password reset request form is completed and the identity of the user has been validated.

6.1.6 All new user's must complete the **Authorisation form (Appendix A)** before being allocated a password in order to ensure that the user comply with the password policy.

6.1.7 If a user's password has expired or the user has forgotten the password, then the user must complete a **Authorisation form (Appendix A)** and send it to ICT Support personnel IT for processing. This is to ensure that all requests to reset passwords are recorded for auditing purposes and to prevent unauthorized resetting of other individual's passwords.

6.1.8 Passwords used within CDM should not be used for external internet accounts and service providers.

6.1.9 No automatic login process to be used.

## 6.2 Password Protection Guidelines

6.2.1 Never write usernames and passwords on keyboards, walls, monitors, post-it notes, tables or any material. A memorized password is not prone to accidental disclosure

6.2.2 Your password is secure and must not be shared with anyone This exempts generic departmental passwords i.e. passwords used and managed by a group in a specific department

6.2.3 New passwords must not be a simple change of the old password e.g. adding a number at the end

6.2.4 Passwords must be changed immediately upon disclosure or suspected disclosure

6.2.5 Certain systems e.g. SAP have specific password requirements over and above those shown above. These systems will prompt the user for the correct information. If in any doubt, contact the Information services for further information.

6.2.6 Computers must be locked when the user moves away from the computer to prevent unauthorized access

## 6.3 Password Construction Standards

**The following table outlines credentials that are applicable to CDM systems and application.**

| No | Credentials | SAP System | Payday systems | Domain Server | Internet | ESS WEB |
|---|---|---|---|---|---|---|
| 1 | Complexity | 8 Character - 3 Number and 4 alphabets<br>1 special character<br>Case Sensitive | | Minimum 7 Alpha/ Numeric Case Sensitive | Windows authentication | Windows authentication |
| 2 | Validity Period | 30 Days | 30 Days | 32 Days | Windows authentication | 30 Days |
| 3 | Attempt Failures | 3 | | 3 | Windows authentication | 3 |
| 4 | Change requests | Authorisation form required | Authorisation form required | Authorisation form required | Authorisation form required | Authorisation form required |
| 5 | Requirement of repetition of passwords | 24 Times | | 12 times | 15 times | 5 Last password |
| 6 | User idle time lockout | 15 minutes | | 15 Minutes | 15 Minutes | 15 Minutes |

## 6.4 Account and Password Protection

A user account will be locked out indefinitely after three failed attempts in order to protect accounts and passwords from brute force attacks or password guessing. Upon account lockout, only the ICT Support personnel can unlock the account at the request of the user involved.

### 6.5 System-Based Password Requirements

Privileged and administrative passwords must be subject to strict composition and frequency of change. Privilege passwords include passwords for routers, switches, firewalls, network operating systems and any other IS resource.

### 6.6 Best Practices for System-Based and Server Passwords

6.6.1 All Passwords must be documented in the password book and kept in the safe at all times. Only authorized personnel must access the safe.

6.6.2 Passwords must be unique for every server

6.6.3 Default factory passwords should be changed immediately after installation.

6.6.4 Accounts created for external contractors should be given restrictive rights to carry out their functions and the accounts should be disabled immediately following the completion of the appointed task

6.6.5 Privileged passwords should not be communicated via telephone, fax, email or any printed form and must not be disclosed to external contractors.

6.6.6 Critical systems for account lockout must be set up to disconnect idle sessions after a period of inactivity of thirty minutes.

6.6.7 Service provider accounts must not rely on admin accounts/passwords.

6.6.8 Systems must be configured to enforce password changes

## 7. Responsibilities

### 7.1 System Administrators

Information security personnel and those that have system administrator roles shall configure CDM information systems to comply with this Password Policy. Information security personnel should work with users in an effort to ensure that they are able to comply with this policy.

### 7.2 Users

Employees, contractors and service providers shall create, maintain and safeguard passwords in compliance to this policy.

### 7.3 ICT Support personnel

ICT Support personnel shall provide, support, develop, enforce and review this policy, and participate in policy exceptions review.

## 8. Exceptions for Non-Compliant Systems and/or Users

Individuals that are unable to comply with the CDM Password Policy must request an exemption from ICT Manager. ICT Manager will process the request for final approval via the policy exceptions review. If after review, there is still disagreement over a decision, it may be appealed to the Municipal Manager. The decision of the Municipal Manager will be final.

## 9. IMPLEMENTATION AND MONITORING

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

## 10. CONSEQUENCES OF NON-COMPLIANCE

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

## 11. 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

## 12. POLICY REVIEW

This policy shall be reviewed as and when required.

## 13. 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

## 14. 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..............................