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.

M.M. Lekganyane

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

RE ŠOMA LE SETŠHABA

CAPRICORN
DISTRICT MUNICIPALITY

ICT ACCOUNT MANAGEMENT POLICY

Policy ref number: 10/5/P-6

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

TERMS AND DEFINITIONS

Account Holder / 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

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 authorised entity

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 unauthorised 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

Guest: Any consultant appointed by the Municipality to render service that requires network access

1. ACRONYM'S AND ABBREVIATIONS

VPN - Virtual Private Network

ID - Identity Document Number/ Password

Email - Electronic mail

CDM - Capricorn District Municipality

ICT - Information and Communications Technology

ISO – Information Security Standards

Cobit – Control Objectives of Information Technology

DEPT – Department

2. PREAMBLE

Information Technology user accounts are one of the primary mechanisms that protect potentially sensitive Municipal network and information resources from unauthorized use. While accounts administration and monitoring are not the most secured way of protecting information and information systems, constructing secure ICT user accounts and ensuring proper password management is essential. Poor ICT user account management and protection can allow both the dissemination of information to undesirable parties and unauthorized access to Municipal network resources.

3. INTRODUCTION

The accepted academic principle that information should be shared is founded upon the fact that information is a unique resource that increases rather than dissipates when it is used. However, this principle must be tempered by the fact that access to Municipal information carries with it the responsibility to protect privacy, confidentiality and integrity.

Unauthorized access to the Municipal information or systems has been identified as a major information security risk that must be proactively managed.

4. PURPOSE

The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to CDM systems. An account, at minimum, consists of a user ID and a password; supplying account information will usually grant access to some set of services and resources. This policy establishes standards for issuing accounts, creating password values, and managing accounts.

5. SCOPE

This policy is applicable to those responsible for the management of ICT network user accounts or access to shared information or network devices. This policy covers Municipal accounts as well as those managed centrally.

6. LEGISLATIVE FRAMEWORK

6.1 ISO (Information Security Standards) 17799
6.2 Information Security Forum (Code of good practice for Information Security)
6.3 Minimum Information Security Standards
6.4 Protection of Information Act
6.5 International Standard for Risk Assessment
6.6 COBIT(Control Objectives of Information Technology) Audit Framework

7. POLICY PRINCIPLES

7.1 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

7.2 Information

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

7.3 Batho pele priniples

Policies developed within CDM will consider all the Batho Pele Principles

8. USER ACCOUNT MANAGEMENT PROCEDURE

8.1 All user accounts used to logon to CDM ICT Network and Information resources 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.

8.2 Authorization form for every allocation must be approved by the Executive Manager of the relevant department

8.3 No external users are allowed to access users profile

9. USER REGISTRATION MANAGEMENT

Accounts that access Municipal ICT network and information resources require prudent oversight. The following security precautions should be part of account management:

9.1 User Registration

9.1.1 The Departmental Managers shall make decisions regarding access to their respective data (e.g., the Manager will determine who has access to which function, and what kind of access each user has). Account setup and modification shall require the signature of the requestor's supervisor.

9.1.2 The Account request form will be used to capture necessary requestor and access information.

9.1.3 Passwords for new accounts shall NOT be emailed to remote users UNLESS the email is encrypted.

9.1.4 The date when the account was issued shall be recorded in an audit log.

9.1.5 All managers of accounts (i.e Municipal officials) with privileged access to all Municipal user accounts shall sign a Confidentiality Agreement (form appearing in Annexure "A")

9.1.6 The user Authorisation request form must be completed. (form appearing as Annexure "B"

9.2 Modification/Changes

9.2.1 The identity of users shall be authenticated before providing them with User account and password details. In addition, it is required that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access.

9.2.2 The user Authorisation request form must be completed for any changes

9.2.3 Whenever possible, passkeys shall be used to authenticate a user when resetting a password or activating a guest account, and should comply with the above standards. Passkeys provide one-time access to a system or application and require the user to change to a password of their choice upon initial login. Where passkeys are not feasible, pre-expired passwords shall be used.

9.2.4 For change of passwords, authorization form can be signed by the immediate supervisor.

9.3 User De-registration

9.3.1 Human Resource will notify IT Department of any Terminations in the Municipality and HR exit form should be filled.

9.3.2 IT Department shall remove or terminate user access on the last day of employment.

9.3.3 Authorization form will be used to terminate user accounts either by removing/disabling/revoking users from any computing system at the end of the individual's employment or when continued access is no longer required.

10. EMERGENCY ACCESS

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

10.2 The following criteria shall be accepted as Emergency Changes

10.2.1 Production loss

10.2.2 Financial loss

10.2.3 Prevention of death

10.2.4 Legislation changes

10.3 Immediate access to the network should be granted and approved by the ICT Manager.

10.4 Created access should be reported with reasons for allocation of emergency access.

11 REVIEW OF USER ACCESS

11.1 All accounts shall be reviewed at least monthly by IT Department official to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status.

11.2 All guest accounts (for those who are not official users of the CDM) with access to Municipal network resources shall contain an expiration date of one year or the work completion date, whichever occurs first.

12. PRIVILEGE MANAGEMENT

12.1 Use of shared accounts shall not be allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g. management of file shares).

12.2 Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

13. USER RESPONSIBILITIES

The cooperation of authorized users is essential for ẹffective security. Users should be made aware of their responsibilities for making effective access controls particularly regarding the use of passwords and the security user equipment.

14. PASSWORD USAGE

14.1 Passwords are a basic control in verifying a user's identity before access is granted to an information system or a service according to the user's authorizations. Each employee shall be responsible for all the actions performed with his/her password, even if it is demonstrated that an action was carried out by another individual using the user's password. Users should therefore follow good security practices in the selection and use of passwords and the following shall be kept in mind:

14.2 Compose passwords that are:

14.2.1 Easy to remember

14.2.2 Of sufficient minimum length

14.2.3 Not based on anything somebody else could easily guess or obtain using person-related information, e.g. names, telephone numbers, dates of birth, etc.

14.2.4 Free of consecutive, identical, all-numeric or all-alphabetic characters.

14.3 Avoid the reuse or cycling of old passwords

15. USER PASSWORD MANAGEMENT

The allocation of passwords shall be controlled through a formal management process and this process should include the following requirements as a minimum:

15.1 If users are required to maintain their own passwords, they shall be provided with a secure initial password, which they should be required to change immediately at first logon.

15.2 Temporary passwords shall be unique and should conform to password standards.

15.3 Users shall acknowledge receipt of passwords.

15.4 Passwords shall never be stored on computer systems in an unprotected form.

15.5 Default vendor passwords shall be replaced as soon as the installation of systems or software has been completed and use designated local administrator password.

15.6 Where technically or administratively feasible, shared ID authentication shall not be permitted.

15.7 Role-based access controls should be used whenever feasible, in order to support changes in staff or assigned duties.

16. MONITORING OF ACCESS USER ACTIVITIES

16.1 Those responsible for access to systems/applications/servers, etc. protected by high-level super-passwords (or the equivalent) shall have proper auditable procedures in place to maintain custody of those "shared secrets" in the event of an emergency and/or should the super-password holder become unavailable.

16.2 These documented procedures, which shall be appropriately secured, should delineate how these passwords are logically or physically accessed as well as who in the "chain of command" becomes responsible for access to and/or reset of the password.

16.3 Activities done by the default account user (i.e. Guest, administrator, owner and root) should be monitored on a daily basis.

16.4 All account logs shall be monitored weekly and administrator must sign log reports.

16.5 After three failed attempts of login a user account will be disabled and the user has to follow the process of password reset. Failed attempts shall be logged unless the log information includes password information

16.6 All inactive accounts for 3 months shall be disabled and it will be activated after a user follows the user account modification/changes.

16.7 Accounts shall be monitored and reviewed

16.8 Password change events shall be recorded in an audit log and signed off by Manager Information Knowledge Management.

17. ENFORCEMENT

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

18. CONSEQUENCES OF NON-COMPLIANCE

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

19 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

20. POLICY REVIEW

This policy shall be reviewed as and when required.

21. 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

22. 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...............................

Annexure 1

CAPRICORN DISTRICT MUNICIPALITY AUTHORISATION, CREATION, CHANGE AND TERMINATION REQUEST FORM

SECTION 1 - Request

Date			
Last Name, First Name		Call Number	
		Telephone Number +)	
Position			
User status	New User __	Existing User __	Department

I. User id Request

Required action (insert X)	Create		Lock Account		Reset Password	
	Change		Unlock Account		Disable Account	
	Delete		Domain User		CDM E-Mail	

Systerm (Mark the applicable)	Development : ____ Quality Assurance : ____ Production/LIVE : ____ Windows Account : ____	ESSWEB: ____ PayDay: ____

Start Date	____/____/____	Expiry Date	____/____/____

II. Authorization Request

Add same Roles as	
Add Role / Profile	
Delete Role/ Profile	
Copy Profile From	
Access Card	

Description / Justification

SECTION 2 – Approval

Requestor

Name & Sig			Date	___/___/_____

Departmental Manager

Name & Sig			Date	___/___/____
Manager IKM				
Name & Sig			Date	___/___/____
System Administrator				
Name & Sig			Date	___/___/____

Annexure 2

CAPRICORN DISTRICT MUNICIPALITY

CONFIDENTIALITY AGREEMENT FORM

All requests for use of IT resources will be governed by the CDM Account Management Policy

This form indicates an authorization for employees that have access to data of information stored on network.

The Municipality is entrusted with or maintains information about its service business operations and ventures. A subset of that information is considered confidential or sensitive, either protected by law, or non-disclosure agreements, or where its exposure could result in the Municipality incurring financial or reputational loss.

To properly safeguard such information, Municipality policy restricts information access and requires all who have access to such information acknowledge that:

- Information entrusted to or maintained by the Municipality will not be disclosed to any individual, group, organization, in order to accomplish legitimate Municipality business.
- A deliberate breach of the above stated confidentiality requirements would be considered a serious infraction of Municipality rule.

Therefore, having been given access to such Municipal information, each individual must sign and date the following confidentiality statement:

- I understand that my access to information entrusted to or maintained by the Municipality is approved solely in conjunction with my assigned duties as an employee of the Municipality and not for any other reason, particularly not for my personal benefit or for the benefit of others.
- I agree that I will take appropriate measures to preserve the confidentiality of this information and not divulge the contents of this information (including any record or report) to any person except in the performance of my work assignment and in accordance with Municipality and departmental policies and procedures, including the Municipality's Information Security Policy.
- I understand that if I do not comply, I will be subject to disciplinary action taken against me.

Official : ______________ Signature: ____________ Date:

IKM Division:________________ Signature: ____________ Date

Senior Manager.: ______________ Signature: ____________ Date