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

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

	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
OFFICE OF THE SPEAKER
2017 -06- 29
LIMPOPO PROVINCE

CAPRICORN
DISTRICT MUNICIPALITY

BACKUP POLICY

Policy ref number: 10/5/P-7

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 policy is defined to address the need for performing periodic computer system backups to ensure that mission critical administrative applications, system data and archives, users' data and archives are adequately preserved and protected against data loss and destruction.

2. DEFINITIONS

2.1 Backup – is the process of copying active files from online disk to tape so that files may be restored to a disk in the event of equipment failure, damage to or loss of data.

2.2 Archive – is the process of moving inactive files form online disk to a tape, i.e. deleting the files from copying them, in order to release online storage for reuse.

2.3 Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

3. ACRONYMS AND ABBREVIATIONS

CDM - Capricorn District Municipality

ICT - Information and Communications Technology

ISO – Information Security Standards

MISS– Minimum information security standard

DHCP - Directory Host Control Protocol

DNS – Domain Name Servers

SAP – Systems Applications Product

4. INTRODUCTION

4.1 Computer information systems and electronic data are valuable assets to Capricorn District Municipality and a substantial investment in human and financial resources has been made to create these systems and information and, as such, a formalized policy has been implemented to:

4.1.1 Safeguard the risk of losing data
4.1.2 Safeguard the confidentiality and integrity of information contained within these systems
4.1.3 Ensure availability of critical data so that information can be utilized as the valuable asset that it is reducing business and legal risk.

4.2 Departmental critical data and non-departmental critical data are stored on File-servers, Exchange-servers (mail-box data) and Application-servers. This data can be categorized as:

4.2.1 Personal User data
4.2.2 Business Unit data
4.2.3 Shared data
4.2.4 Databases
4.2.5 Application / System data

5. PURPOSE AND OBJECTIVES

To provide secure storage for data assets critical to the work flow of the Municipality

To prevent loss of data in the case of accidental deletion / corruption of data, system failure, or disaster

To permit timely restoration of archived data in the event of a disaster or system failure

6. SCOPE

The scope is to ensure that departmental data can be recovered within required and agreed business timescales.

This policy applies to all computers, both mobile and desktop, owned by the Municipality

7. LEGISLATIVE FRAMEWORK

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

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

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

8. POLICY PRINCIPLES

8.1 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

8.2 Information

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

8.3 Batho pele priniples

Policies developed within CDM will consider all the Batho Pele Principles

9. RESPONSIBILITIES

9.1 ICT Department is responsible for backing up File-servers, Exchange servers and Application-servers, according to agreed cycles, and storing these backups in a secure designated area.

9.2 In addition to backing up departmental data, the Department shall perform regular disk capacity management on all data servers and have the right to delete all non-departmental related data after consultation with involved employees.

9.3 If the disposal of old or damaged tapes is required, such tapes will be destroyed to prevent the recovery of data from the media.

9.4 Ownership of all electronic information residing on any departmental computer system vests in Capricorn District Municipality and Management may peruse, monitor and take copies of any information or communication made or received utilizing any of the aforementioned

systems. Therefore, ICT department requires that all requests to restore an employees user data, residing on File-servers or Exchange-servers (mail-box data), not requested by the employee or without the permission of such employee, must be authorized by Executive Manager and may be assessed by the Manager ICT.

10. DATA BACKED UP

10.1 Windows Backup

10.1.1 System State backup
- a) DHCP (Directory Host Control Protocol)
- b) DNS (Domain name Settings)
- c) Security log
- d) User files
- e) Shared folder

10.1.2 Incremental daily
10.1.3 Daily onsite/offsite – Mirrored offsite
10.1.4 Data restoration – as and when data is required to be restored

10.2 SAP (System Applications Product)

10.2.1 Backup full database
10.2.2 Full back up to a disk
10.2.3 Data synchronization off three systems – Development, Quality Assurance and Production
10.2.4 Backup Restore – through data synchronization
10.2.5 Backup tapes kept offsite

10.3 Payday

10.3.1 Backup of data files incorporated with the daily online/offsite full backup.
10.3.2 Restore test to be done annually.

10.4 ESS Database

10.4.1 Daily incremental tape backup
10.4.2 Weekly backup media moved offsite once a week during site rotation
10.4.3 Restore test as and when data is required to be restored

11. EXCLUDED EXTENSIONS

On **home directories folders ("My Documents")** not all files will be backed up; the following are extensions that will be omitted:

7.1 Mpeg
7.2 Mpa
11.1 Mp2
11.2 Mp3
11.3 Mp4
11.4 Exe
11.5 Vob
11.6 Wsf
11.7 Wma
11.8 Wav

12. TAPE STORAGE

All weekly and monthly tapes must be stored on the fire proof safe at the remote site.

13. TAPE DRIVE REPLACEMENT

Tape drive shall be cleaned monthly and the cleaning tape shall be replaced every 6 months.

14. RESPONSIBILITIES

14.1 ICT Department

The ICT Manager shall delegate a member of the User Support division to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis. The designated person will take weekly and monthly tapes to offsite storage.

14.2 The Employee

All business critical data on local computer and notebook hard drives must be copied or moved to a "My Documents" on a file server, where it will be backed up. Where such an action is not possible, as in cases where it is done away from access to Capricorn District Municipality network, the data must be copied over on

the first available opportunity. It will be the sole responsibility of the employee, under all circumstances, to backup and maintain security regarding personal data.

15. RESTORATIONS

Users that need files restored must submit a request to the IT help desk by completing Data Restore Request Form.
Information regarding the request where possible must include the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

16. REPORTS

An automated backup report on required system should be kept and managed properly. All failed backup should be reviewed

A register to be kept on all tape backup done for systems

17. IMPLEMENTATION AND MONITORING

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.....