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

RE ŠOMA LE SETŠHABA

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
DATA CENTER ACCESS CONTROL AND ENVIRONMENTAL POLICY
Policy ref number: 10/5/P-8

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 Contents

1. PREAMBLE

Data Centres are found in almost all organisations ICT infrastructure. These data centres host the server environment and electronic data. Due to the sensitivity nature of these data centres, a policy is imperative to guide the Department on the proper mechanisms to manage this room as well to protect information.

2. DEFINITIONS

Access Control: Mechanisms and policies that restrict access to resources.

AC: Alternating Current - an electrical current that frequently reverses direction.

CCTV: Closed Circuit Television is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

Data Centre: facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.

Fire Extinguishers: an active fire protection device used to extinguish or control small fires, often in emergency situations.

Raised floor: Types of floor that provide an elevated structural floor above a solid substrate (often a concrete slab) to create a hidden void for the passage of mechanical and electrical services.

Tailgating: Entering an area without authorisation verification by following someone who has access.

UPS: an electrical apparatus that provides emergency power to a load when the input power source, typically mains power, fails

ACRONYMS AND ABBREVIATIONS

CDM - Capricorn District Municipality

ICT - Information and Communications Technology

ISO – Information Security Standards

Cobit – Control Objectives of Information Technology

DEPT – Department

MB - Megabyte

UPS – Uninterruptable power supply

3. INTRODUCTION

Data Centres are found in almost all organisations ICT infrastructure. These data centres host the server environment and electronic data. Due to the sensitivity nature of these data centres, a policy is imperative to guide the Department on the proper mechanisms to manage this room as well to protect information

4. PURPOSE

The purpose of this document is to define the policies and procedures relating to access control, environmental control, and operations of Capricorn District Municipality Data Centre.

5. SCOPE

The scope of the policy will cover, but is not limited to the following areas:

5.1 Security
5.2 Safety measures and procedures
5.3 Emergency measures and procedures
5.4 Access control procedures
5.5 Change and configuration management
5.6 Environmental control, reporting and maintenance
5.7 Monitoring facilities.

6. LEGAL MANADATES

6.1 Information Security Forum (The standard of good practice for Information Security)
6.2 Minimum Information Security Standards
6.3 Copyright Act
6.4 Protection of Information act
6.5 Promotion of Access to Information Act of 2000

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. SECURITY

8.1 Background

8.1.1 The vulnerability of business critical information systems and the data they contain within the Data Centre make the site a high value asset, which requires a high degree of protection.

8.1.2 A range of security measures are therefore in place to protect employees, information and physical assets, along with the reputation of CAPRICORN DISTRICT MUNICPALITYand interested third parties with equipment in the Data Centre.

8.2 Entry Systems and Access Control

8.2.1 Access shall be controlled access control and burglar doors

8.2.2 Staff and visitors shall not adjust or otherwise tamper with door fittings. Any suspected faults with doors, lights or any security equipment should be reported to IT Manager immediately.

8.2.3 Any person other that IT staff requiring access to the Data Centre shall sign the log book located within the upper ground security reception area upon arrival.

8.2.4 Only authorised IT and Security Services personnel shall have access to the Data Centre access control system. Any other personnel including full time employees, contractors and vendors will be escorted by authorised IT and/or Security personnel during office hours.

8.3 Contractor Access After Hours

8.3.1 Security Services shall be responsible for access control and security of the Data Centre outside normal working hours.

8.3.2 In case where contractors require access to Data Centre after hours, Security Services shall be responsible to provide such access and protection.

8.3.3 The IT Manager will authorise the use and changes to be made in the Data Centre.

8.4 Close circuit television

8.4.1 Internal, entry and exits area of the Data Centre shall be monitored by a closed circuit television (CCTV) to capture all Data Centre activities.

8.4.2 CCTV shall be integrated and monitored by Security Services.

9. SAFETY

91 Overview

In addition to the safety precautions outlined herein, the Data Centre safety precautions shall be applied in conjunction with Capricorn District Municipality Occupational Health and Safety policy.

9.2 Signs and information

9.2.1 Safety signs and information shall be posted at access points to the Data Centre.

9.2.2 General notices shall also be posted around the Data Centre; providing detailed information on first aid, emergency contacts and general Health and Safety issues

9.3 Emergency Exits and Fire Alarm Procedures

9.3.1 When fire alarm is triggered at the Data Centre, normal emergency procedures shall be followed as stipulated by Capricorn District Municipality emergency evacuation procedures. Lifts shall not be used; only emergency stair ways shall be used.

9.4 Fire Detection and Fire Extinguishers

9.4.1 Fire and smoke detection system shall be fitted and linked to audible and virtual alarms.

9.4.2 If an alarm is activated the Data Centre shall be evacuated immediately to avoid gas inhalation and the incident shall be reported to Security Services and or IT Manager.

9.5 Electrical Safety

9.5.1 Only qualified electrical technicians shall have access to electrical systems, IT staff and other personnel should contact the relevant electrical personnel when encountering electricity problems.

9.5.2 Request shall be authorised by the IT Manager.

10. DATA CENTRE USE

10.1 Hours of Operation

10.1.1 The Data Centre will be operated during office hours to authorised personnel between 7:45 am to 16:30 pm.

10.1.2 Access afterhours for maintenance purposes will be authorised and delegated by the ICT Manager.

10.2 Equipment Delivery

10.2.1 Delivery of equipment shall be supervised by authorised personnel upon approval by the ICT Manager.

10.3 Control of Equipment and Spares

10.3.1 No unused equipment and spares shall be left at the Data Centre.

10.3.2 Alternate storage facility shall be available for such purpose.

10.4 Prohibited Items

The following items are prohibited from the Data Centre:

10.4.1.1 Combustible materials such as paper and cardboard (except reference manuals as needed);

10.4.1.2 Food and drink;

10.4.1.3 Tobacco products;

10.4.1.4 Explosives and weapons;

10.4.1.5 Hazardous materials;

10.4.1.6 Alcohol, illegal drugs and other intoxicants;

10.4.1.7 Electro-magnetic devices that could cause interference with computer and telecom equipment;

10.4.1.8 Radioactive materials; and

10.4.1.9 Photographic or recording equipment (other than backup media).

10.5 Cables and Wiring

10.5.1 Cables and wires shall be structured and labelled when running under the raised floor, wall, and equipment racks.

11. ENVIRONMENT

11.1 Air Conditioning

11.1.1 Air conditioning shall be provided in the Data Centre.. It shall deliver enough cooling per rack in accordance with design specification.

11.1.2 Service shall be done at least three times a year by a reputable maintenance service provider for Airdale equipment. Certificate for maintenance performed shall be submitted to the Municipality.

11.2 CO2 Fire Extinguisher

11.2.1 Class E gas fire extinguisher shall be implemented to prevent damage to Data Centre electrical facilities.

11.2.2 Service shall be done at least annually by a reputable maintenance service provider for C02 gas shall be done. Certificate for maintenance performed shall be submitted to the Department.

11.3 Power and lighting Provisioning

11.3.1 Two single phase power sockets shall be available in each rack and shall be fed directly from the main switch.

11.3.2. Adequate power light shall be available to ensure that all equipments in the Data Centre are clearly visible.

11.3.3 Lights shall be switched off when no access to the Data Centre is required.

11.4 UPS Provisioning

11.4.1 All major equipment at the Data Centre shall be powered on by a UPS system, should the AC power goes down. The UPS system should sustain power to those devices for at least 10 minutes to allow graceful shutdown.

11.4.2 Service shall be done at least annually by a reputable maintenance service provider for APC Galaxy equipment. Certificate for maintenance performed shall be submitted to the Department.

11.5 Environment Monitoring

11.5.1 A number of monitors shall be put in place to report on issues affecting the Data Centre environment. Monitoring system shall report to designated IT and Security personnel

11.5.2 Monitoring shall include:

11.5.2.1 Fire and Smoke Detectors;

11.5.2.3 UPS malfunctioning or discharge during normal AC power operation;

11.6 Dust Prevention

11.6.1 The Data Centre shall be well ventilated to prevent dust from affecting equipments.

11.6.2 Equipment to be installed in the Data Centre shall be dust freed outside before introduced in the Data Centre.

11.7. Waste Disposal and Cleaning

11.7.1 Cardboard and other items that can generate dust and that are easily combustible should remain outside the Data Centre.

11.7.2 Waste bin shall be available outside the Data Centre main entrance for easy disposal of other items of waste.

12. CHANGE AND CONFIGURATION MANAGEMENT

12.1 The IT Manager is responsible for all changes that shall take place at the Data Centre

12.2 All changes to be made shall be requested to and authorised by the IT Manager.

12.3 The Manager will monitor and review the Data Centre access log book on a regular basis.

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...............................