

094847

# EPHRAIM MOGALE LOCAL MUNICIPALITY

☎ 111  
MARBLE HALL  
0450  
☎ 013-261 8400  
☎ 013-261 2985



Leeufontein Office (013) 266 7025  
Elandskraal Office (013) 268 0006  
Zamenkomst Office (013)973 9160  
Traffic Section (013) 261 8400

EXTRACTS FROM THE MINUTES OF THE 3<sup>RD</sup> ORDINARY COUNCIL MEETING OF  
EPHRAIM MOGALE LOCAL MUNICIPALITY HELD ON WEDNESDAY THE 29<sup>TH</sup> APRIL  
2015

FILE/S: ~~8/4/P~~ 6/2/2/P

OC3/15/2015 INFORMATION COMMUNICATION TECHNOLOGY (ICT) RELATED  
POLICIES ~~8/4/P [00/02/P]~~

## RESOLVED

1. That the Council takes cognizance of the circulated report.
2. That the Council approves the following ICT related policies and procedures:
  - 2.1 Account Management Policy.
  - 2.2 Change Management Procedure.
  - 2.3 End User Management Policy.
  - 2.4 Patch Management Policy.
  - 2.5 User Management Procedure.
  - 2.6 ICT Global Policy.
  - 2.7 ICT Security Policy.
3. That the Council approve the reviewal of the following policies and procedures:
  - 3.1 Back up Policy & Procedure.
  - 3.2 Allocation of Movable ICT Devises Policy & Procedure.
4. That the Council refer the policies to the LLF.
5. That the approved policies and procedures be implemented with effect from the 1<sup>st</sup> April 2015
6. That there be a clear policy that distinguish the ownership of the i-pad equipment carried by Councillors,
7. That the Council instruct the Municipal Manager to implement the decision accordingly.

**L.B. MODISHA  
SPEAKER**

**29 APRIL 2015**

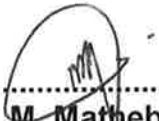
## **FINALISATION BY:**

ALLE KORRESPONDENSIE MOET AAN DIE  
MUNISIPALE BESTUURDER GERIG WORD

MANGWALO KA MOKA A LEBANTSHWE  
GO MOLAODI WA MASEPALA

ALL CORRESPONDENCE TO BE ADDRESSED  
TO THE MUNICIPAL MANAGER

Referred to Director Corporate Services by Municipal Manager



M.M. Mathebela  
Municipal Manager

05/05/15

Date Received

## **PURPOSE**

For the Council to approve of the attached ICT policies.

## **BACKGROUND**

Ephraim Mogale Local Municipality is an ICT environment as most of our administrative activities are carried out through the utilization of computers and network systems. It therefore becomes necessary to have policies to regulate the utilization of this important tool and yet vulnerable to misuse and abuses that may have detrimental consequences.

The policies further aims to regulate access to the municipal network, possibly from when a new employee comes into the system and when he/she leaves the institution.

The various attached policies in brief aims to cover inter alia the following:

- Establishing a standard for the administration of computing accounts that facilitate access or changes to the Ephraim Mogale Local Municipality. 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, resetting password and managing accounts.
- regulating the implementation of changes in the current systems prompted by upgrades and the vital changes in systems technology used in the Municipality.
- establishing ethical guidelines for Ephraim Mogale Local Municipality's ICT users, assets and computing facilities.  
(ICT assets include desktop computers, desktop components, laptops, servers, switches, routers, printers, photocopiers, phones, 3G, Tablets, email, internet, mobile modems, firewall, software, business applications, municipal data and information).
- Describing the requirements for maintaining up-to-date operating system security patches on all Ephraim Mogale local municipality owned and managed workstations and servers.
- Procedure for the creation of new users on the system.
- regulating the use of ICT assets, provides guidelines, roles and responsibilities for acceptable use, prescribe minimum requirements for acceptable use, provides guidelines on the protection against unauthorized access, provides measures to safeguard intentional or unintentional loss of information and provides measures for adequate security protocols.
- Cover the ICT security,
- Addressing the procedures for backup.
- Regulate the allocation of movable ICT devices.

**They are as follows:**

1. Account Management Policy.
2. Change Management Procedure.
3. End User Management Policy.
4. Patch Management Policy.
5. User Management Procedure.
6. ICT Global Policy.
7. ICT Security Policy.
8. Back up Policy & Procedure.
9. Allocation of Movable ICT Devices Policy & Procedure.

**RECOMMENDATIONS OF THE EXECUTIVE COMMITTEE**

1. That the EXCO takes cognizance of the circulated report.
2. That the Council approves the following ICT related policies and procedures:
  - 2.1 Account Management Policy.
  - 2.2 Change Management Procedure.
  - 2.3 End User Management Policy.
  - 2.4 Patch Management Policy.
  - 2.5 User Management Procedure.
  - 2.6 ICT Global Policy.
  - 2.7 ICT Security Policy.
3. That the Council approve the reviewal of the following policies and procedures:
  - 3.1 Back up Policy & Procedure.
  - 3.2 Allocation of Movable ICT Devices Policy & Procedure.
4. That the Council approves that the reviewed policies replaces any other policy that existed prior the reviewal of the policies.
5. That the approved policies and procedures be implemented with effect from the 1<sup>st</sup> April 2015
6. That the Council instruct the Municipal Manager to implement the decision accordingly.

**RECOMMENDATIONS OF THE PORTFOLIO COMMITTEE**

1. That the Committee takes cognizance of the circulated report.
2. That the Council approves the following ICT related policies and procedures:
  - 2.1 Account Management Policy.
  - 2.2 Change Management Procedure.
  - 2.3 End User Management Policy.
  - 2.4 Patch Management Policy.
  - 2.5 User Management Procedure.
  - 2.6 ICT Global Policy.
  - 2.7 ICT Security Policy.
3. That the Council approve the reviewal of the following policies and procedures:

- 74
- 3.1 Back up Policy & Procedure.
  - 3.2 Allocation of Movable ICT Devices Policy & Procedure.
  4. That the Council approves that the reviewed policies replaces any other policy that existed prior the reviewal of the policies.
  - 5 That the approved policies and procedures be implemented with effect from the 1<sup>st</sup> April 2015
  6. That the Council instruct the Municipal Manager to implement the decision accordingly.

### **RECOMMEND TO RESOLVE**

1. That the Council takes cognizance of the circulated report.
2. That the Council approves the following ICT related policies and procedures:
  - 2.1 Account Management Policy.
  - 2.2 Change Management Procedure.
  - 2.3 End User Management Policy.
  - 2.4 Patch Management Policy.
  - 2.5 User Management Procedure.
  - 2.6 ICT Global Policy.
  - 2.7 ICT Security Policy.
3. That the Council approve the reviewal of the following policies and procedures:
  - 3.1 Back up Policy & Procedure.
  - 3.2 Allocation of Movable ICT Devices Policy & Procedure.
4. That the Council approves that the reviewed policies replaces any other policy that existed prior the reviewal of the policies.
- 5 That the approved policies and procedures be implemented with effect from the 1<sup>st</sup> April 2015
6. That the Council instruct the Municipal Manager to implement the decision accordingly.

EPHRAIM MOGALE LOCAL MUNICIPALITY



ACCOUNT MANAGENT POLICY

**DOCUMENT APPROVAL**

Responsible Person:	Name	Signature	Date
	Mathebela M.M.		18/06/15

Date of approved: 29 April 2015

42

1. **Preamble**

ICT user accounts are one of the primary mechanisms that protect potentially sensitive departmental network and information resources from unauthorized use. While accounts administration and monitoring are not the only 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 departmental network resources.

2. **Terms and definitions**

**Account Holder / User:** Any person granted an ICT user account with the Municipality

**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,

**User:** Any person using any of the Department's Information Technology Facilities,

**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,

**VPN:** Virtual Private Network,

**ISO:** Information Security Officer,

### **3. Purpose**

The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to the Ephraim Mogale Local Municipality. 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, resetting password and managing accounts.

### **4. 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 departmental accounts as well as those managed centrally.

### **6. User Account Management Procedure**

All user accounts used to logon to the Ephraim Mogale Local Municipality 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.

### **7. User Registration Management**

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

#### **7.1 User Registration and Deregistration**

7.1.1 Human Resources shall accordingly notify ICT section of the employed personnel, then a network registration form shall be completed by the incumbent with the approval of the Director or Manager of the division which the incumbent report to, (e.g., manager will determine who has access to certain programs and application, and what kind of access each user should have has). Account setup and modification shall require the signature of the requestor's supervisor.



The "Network Registration form" shall be available in the user's personal file, ICT office and records.

- 7.1.2 The identity number, full names of the applicant, department and the signature of the immediate supervisor will be required to register a user on to the Ephraim Mogale Local Municipality's network.
- 7.1.3 Passwords for new accounts shall NOT be given to user department.
- 7.1.4 When establishing accounts, standard security principles of "least required access" to perform a function shall always be used, where administratively feasible. For example, a root or administrative privileged account must not be used when a non-privileged account will do.
- 7.1.5 In the event an employee resigns from the employment of Ephraim Mogale Local Municipality the Human Resource division shall accordingly notify the ICT division to process deactivating the employee from the Municipal network accordingly upon completion of notice period.

## **7.2 Modification/Changes**

- 7.2.1 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 without any administrative rights.
- 7.2.2 A "Request of reset password form" that can be accessible from the ICT Office.
- 7.2.3 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.

## **7.3 User De-registration**

- 7.3.1 ICT division shall issue a unique ICT user account with a standard of initial & surname to each individual authorised to access the departmental network and information resources. ICT SECTION is also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.

## **8. Review of User Access**

- 8.1 All accounts shall be reviewed at least annually by ICT SECTION official to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status.

8.2 All guest accounts (for those who are not official users of the Ephraim Mogale Local Municipality) with access to the Ephraim Mogale Local Municipality network resources shall contain an expiration date of one month or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

## 9. Privilege Management

9.1 For access to sensitive information managed by a department, only the relevant personnel shall have access to that system and each user should have his/her individual password.

9.2 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). Such exceptions will require documentation which justifies the need for a shared account.

## 10. User Responsibilities

The cooperation of authorized users is essential for effective 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 and also keeping the passwords a secret.

## 11. Password Usage

Password are used for various purposes. Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, voicemail password and local router logins. Since very few systems have support for one time tokens (i.e dynamic password which are only used once), everyone should be aware of how to select strong password.

Poor, weak password are identified by having the following characteristics:

- password contains less than six characters.
- Password contains common usage word such as:
- names of family, pets, friend, co-worker, fantasy characters, etc.
- computer terms and names, commands, sites, companies, hardware, software, etc.
- birthdays and other personal information such as addresses and phone numbers.
- words or numbers patterns like aaaabbb, qwert, 123321, etc.
- words patterns preceded by a digit (e.g secrete1, 1secrete).

Strong password are identified by having the following characteristics

- contains both upper and lower case characters such (e.g a-z, A-Z).
- have digits and punctuation characters as well as letters (e.g 0-9, #,\$@\*^>).
- are at least six alphanumerical characters long and is a passphrase.

- are not a works in any language, slang, dialect, jargon, etc.
- are not based on personal information, names of family etc.
- password should never be written down or stored on line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.
- Password should be in an alpha numeric form.

### **11.1 Password protection Standards and management**

Do not use the same password for Ephraim Mogale Local Municipality accounts and other non-Municipal access such as personal ISP account.

Where possible do not use the same password for various Municipal access needs, select one password for each access needs.

Do not share your password with anyone, including supervisors, managers and secretaries, all password are to be treated as sensitive and confidential information.

#### **THINGS NOT TO BE DONE**

- Reveal a password over the phone to anyone.
- Reveal a password via an email.
- Talk about a password in front of others.
- Hint at the format of the password.
- Share password with family members.
- Reveal password to co-workers while on vacation.
- Do not write down and store password and store them in your office and never store such a password in a file on any computer without encryption

#### **THINGS TO DO**

- Change password on monthly basis
- In the event an account is suspected to have been compromised, it must be reported immediately and be changed.

Password cracking or guessing shall be performed on a periodic or random basis, should the password be cracked the user shall be required to change it.

## **12. Monitoring of access user activities and handling inactive users**

- 12.1 Access to systems/applications/servers, etc. shall be managed by Administrator account and the password shall be known only by ICT division.
- 12.2 Activities done by the default account user (i.e. Guest, administrator, owner and root) should be monitored on a daily basis.
- 12.3 After three failed attempts of login a user account will be locked, the process of changing a password will be followed.

- 12.4 All inactive accounts for ONE (01) month shall be disabled and it shall be activated after a user follows the user account modification/changes.
- 12.5 All accounts that are inactive for THREE (03) months shall be deleted from the systems
- 12.6 Accounts shall be monitored and reviewed from time to time.
- 12.7 Password change shall be recorded in the ICT division upon completion of relevant password reset form.

**13. Exceptions for Non-Compliant Systems and/or Users**

Individuals that are unable to comply with the Ephraim Mogale Local Municipality Account & Password Management Policy must request an exemption from ICT division. ICT division shall 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 Manager ICT division. The decision of the Manager ICT division will be final.

**14. Enforcement**

ICT division is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

**15. Consequences of Non-Compliance**

Non-compliance of this policy may lead to disciplinary actions, legal liability when found guilty.

**16. Policy Review**

This policy shall be reviewed on a need basis.

**16. Implementation**

This policy comes into effect from the date of approval.



EPHRAIM MOGALE LOCAL MUNICIPALITY

NETWORK REGISTRATION FORM

DETAILS

Name		Initials	
Surname		Title	
ID. No.			
Position			
Department			
Email		Contact	
Office			
Employment Type	Permanent Employee	<input type="checkbox"/>	
	Temporary Employee	<input type="checkbox"/>	
	Internship	<input type="checkbox"/>	Period: _____
	Volunteer	<input type="checkbox"/>	Period: _____
	Service Provider	<input type="checkbox"/>	Name: _____

OFFICE USE ONLY

Password			
User Context			
Date added on the Domain			
Added by (ICT Official)			
Desktop	S/N:	Laptop	S/N:
Printer	S/N:	Other	S/N:

Supervisor Signature

DECLARATION

I, \_\_\_\_\_ agree that the above given information is correct. I acknowledge and accept that all data & equipment stored on Municipal computers is the property of the Municipality. All Documents that belongs to the Municipality must always be saved on the network. When I leave the Municipality I will return all equipment & software issued to me.

Signed at \_\_\_\_\_ day of \_\_\_\_\_ month of \_\_\_\_\_ year 20\_\_



EPHRAIM MOGALE LOCAL MUNICIPALITY

PASSWORD RE-SET /UNLOCK FORM

INITIALS	
NAME	
SURNAME	
DEPARTMENT	
E-MAIL ADDRESS	
CELL NO	
PASSWORD TYPE	<input type="checkbox"/> MUNSOFT <input type="checkbox"/> WINDOWS <input type="checkbox"/> VIP
EASON:	

**DECLARATION**

I, \_\_\_\_\_ agree that the above given information is correct.  
I acknowledge that the re-set of password is according to the Municipal ICT Policy.

\_\_\_\_\_  
Signature: ICT Official

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature: User

\_\_\_\_\_  
Date