

094847

EPHRAIM MOGALE LOCAL MUNICIPALITY

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



Leeuwfontein 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 3RD ORDINARY COUNCIL MEETING OF
EPHRAIM MOGALE LOCAL MUNICIPALITY HELD ON WEDNESDAY THE 29TH 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 1st 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

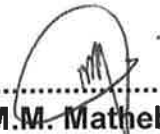
FINALISATION BY:

ALLE KORRESPONDENSIE MOET AAN DIE
MUNISIPALE BESTURDER 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 devised.

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 Devises 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 Devises 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 1st 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:

- 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 1st 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 1st April 2015
 - 6. That the Council instruct the Municipal Manager to implement the decision accordingly.

EPHRAIM MOGALE LOCAL MUNICIPALITY



PATCH MANAGEMENT POLICY

DOCUMENT APPROVAL

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

Date of approved: 29 April 2015

1. OVERVIEW

Ephraim Mogale local municipality is responsible for ensuring the confidentiality, integrity, and availability of data stored on its systems. Ephraim Mogale local municipality has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

2. PURPOSE

The policy describes the requirements for maintaining up-to-date operating system security patches on all Ephraim Mogale local municipality owned and managed workstations and servers.

3. Definitions

Term	Definition
Patch	A piece of software designed to fix problems with or update a computer program or its supporting data
Trojan	A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
Worm	A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.
WSUS	Windows Server Update Services (WSUS), is a computer program developed by Microsoft Corporation that enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in a corporate environment.

4. SCOPE

The policy applies to workstations or servers owned or managed by the municipality, this includes systems that contain Municipal data regardless of their location.

- Microsoft Windows servers
- Workstations (desktops and laptops)

5. POLICY

Workstations and servers owned by Municipality must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers of the Municipality.

5.1 Workstations

5.1 Workstations

Desktops and laptops shall have automatic updates enabled for operating system patches. This shall be the default configuration for all workstations of the Municipality and shall be managed by the ICT division.

5.2 Servers

Servers must comply with the minimum baseline requirements that have been approved by the Municipality. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Municipal asset and the data that resides on the system.

6. MONITORING AND REPORTING

- WSUS shall be the system used to monitor and deploy the patches on the Municipal network.
- Patches shall be managed at a central point by ICT division.
- ICT Division shall be responsible for monitoring the process of deploying patches.
- Users shall not be permitted to interrupt the system during the deployment of patches.
- All Desktop/Laptop shall report to WSUS which shall give full status about the system.
- All Laptop users shall be responsible for attaching the system to the Municipal network regularly.

6.1 Anti virus

All Municipal workstation computers must have standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified and declared as virus-free. ICT Division is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified and declared as virus-free.

Any activities intended to create and/or distribute malicious programs into Municipal networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

6.2 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all employees of Ephraim Mogale local Municipality. ICT division reserve the rights to conduct random assessments to ensure compliance with policy without prior notice.

7. IMPLEMENTATION

The policy become effective upon approval, and shall be reviewable on a need basis.