9i

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 TECHNOCLOGY (ICT) RELATED POLICIES ~~8/4/P [06/02/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.

LBModisha
L.B. MODISHA
SPEAKER

29 APRIL 2015

FINALISATION BY:

Referred to ...Director Corporate Services.............by Municipal Manager

....
M.M. Mathebela
Municipal Manager

05/05/15.
....
Date Received

OC3/15/2015 INFORMATION COMMUNICATION TECHNOCLOGY (ICT) RELATED POLICIES 8/4/P [06/02/P]

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 PORTFOKLIO 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 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.

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 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.

12

EPHRAIM MOGALE LOCAL MUNICIPALITY

ICT BACK UP POLICY

DOCUMENT APPROVAL

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

Date of approved: 29 April 2015

1. Overview

This document defines the backup policy for all data within the Municipality. The data typically includes that which resides on servers, desktops, laptops & other storage or processing devices that is critical to the operation of the Municipality.

2. Purpose

Data backup is critical to ensure the continued operation of a business in the event of equipment failure, natural disasters or intentional destruction. The purpose of this document is to provide parameters within which ICT personnel must operate to ensure the safe and reliable backing up of business critical data.

3. Scope

This policy applies to all data owned by the Municipality that is critical to the successful operation of the business. Not covered in this document are any guidelines or policies relating to Disaster Recovery.

4. Definitions

- **Backup** - The saving of files onto magnetic tape or other offline mass storage media or online storage for the purpose of preventing loss of data in the event of equipment failure or destruction.
- **Archive** - The saving of old or unused files onto magnetic tape or other offline mass storage or online storage media for a specified period per set archiving standard.
- **Restore** - The process of bringing data back from the storage media back into the live system or test system.
- **Disaster Recovery** – The short term provisioning of systems and data to aid in business continuity in the event of a major equipment failure or natural or human induced disaster.
- **Emergency Restore** – Data loss that will result in direct or indirect financial, reputational damage is deemed grounds to implement an Emergency Restore.
- **Power User** – High level users (Directors, CFO, etc and others as identified by the IT Manager)
- **Selection List** – Data deemed essential to the business as defined by the organisation

5. Frequency (Servers)

5.1 Full backups shall be performed:

- Electronically on daily basis and shall run after 20:00 and complete before 07:00 and a subsequent report generated to determine the success or failure of the backup.

5.2 Reporting & Monitoring:

- Monitoring of backup success or failure shall be performed on daily basis, and a report received electronically.

- A consolidated monthly and quarterly backup report shall be generated by the service provider and sent to the Municipality's ICT section for scrutiny.
- The system shall be tested at least once (01) in six months and a system test certificate shall be sent to the ICT section of the Municipality.

6. Exceptions

6.1 Backup exceptions shall include but not limited to:

- Failure to start
- Failure to complete before 7:00
- Complete with warnings
- Complete with errors

Should any of the above events occur, ICT section shall ensure the following actions are implemented:

- Log the incident in the ICT incident tracking system.
- Advise the affected department.
- Manually perform the backup process.
- Perform continuous troubleshooting to ensure backup success.
- Ensure exception is documented with remedial action taken to resolve exception.
- Follow up on each incident logged to ensure no exception is repeated.

7. Retention & Archiving

7.1 Data retention shall be designed according to regulatory requirements,

7.2 Backed up data shall reside offsite at an appropriately secured environment that complies with the required distance, to ensure that in the event the live/primary site is struck by disaster, backed up data must remain available and accessible.

8. Responsibility

The ICT division manager remains accountable and may in writing delegate a member from the ICT section to perform regular backups monitoring and reporting.

9. Selection List

9.1 Financial Management Data

- Current live database
- Current live data
- Server system state

9.2 Human Resources & Payroll Data

- Payroll databases (current and historical)
- Server system state

9.3 Domain Controller

- Server system state

9.4 Emails

- Log files
- Server system state
- Mail stores (collaborator)

9.5 File Server

- Server system state
- Data

9.6 Application Server

- Application(s) current live database
- Application(s) current live data

9.7 Desktop & Laptop

- Documents and Settings
- Users

9.8 Default exclusions\filters unless specified:

- Personal archive mail files such as (but not limited to) .pst, .ost
- Video files such as (but not limited to) .wmv, .avi, .mov,.mkv, .mp4
- Audio files such as (but not limited to) .mp3, .wav, .ogg, .wma
- Images such as (but not limited to) .jpg, .tiff, .jpeg, .bmp
- Executable files such as (but not limited to) .exe, .bat, .com, .msi, .pkg

10. Restoration & Testing

10.1 Restoration of files:

Users that requires files to be restored shall submit a written request to the ICT section.

10.1.1 The file restoration requisition shall be completed and inclusive of information about the file creation date, the name of the file, the last time it was changed, and the date and time it was destroyed, the process shall be authorized by the appropriate supervisor of the requesting user.

10.2 System Restore:

10.2.1 In the event there be a system failure where an emergency restore is required, the system administrator may restore the necessary data and then later document the restore and test thereof and have the documentation approved by the supervisor of the affected section.

10.2.2 All application data and User Data shall be restored according to the restore procedure to test and ensure that the backed up data is still in working condition and that backup was full successful.

10.3 Testing:

10.3.1 The ability to restore data from backups shall be tested as per the application/system set rules. A system test certificate shall be issued.

10.3.2 Restore tests are performed as per agreed schedule of service and are signed off by a designated official from ICT section.

10.3.3 In the event of test failure, the failure must be logged in the appropriate incident tracking system and Root Cause Analysis provided. This RCA will be used to prevent repeat of failure. Once the incident is resolved, the restore test must be run to successful completion.

11. Implementation

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