

# ELIAS MOTSOLEDI LOCAL MUNICIPALITY-MASEPALA WA SELEGAE



## PHYSICAL SERVER ROOM ACCESS POLICY

MUNICIPAL COUNCIL RESOLUTION NUMBER

M24/25-07

APPROVED AT THE 1<sup>ST</sup> ORDINARY COUNCIL SITTING OF 30 AUGUST 2024

## Table of Contents

1. Glossary of terms .....	2
2. Introduction .....	3
3. Policy Statement... ..	3
4. Purpose .....	3
5. Related policies, processes and procedures .....	4
6. Scope .....	4
7. Policy application.....	4
8. Roles and responsibility .....	4
9. Procedure.....	4
10. Compliance .....	8
11. Administration of the policy .....	8
12. Policy implementation... ..	8
13. Updating the policy .....	8
14. Policy review .....	8
15. Effective date... ..	8
16. Signatories.....	9



## 1. GLOSSARY OF TERMS

EMLM	ELIAS MOTSOLEDI LOCAL MUNICIPALITY
MM	MUNICIPAL MANAGER
SA	SYSTEM ADMINISTRATOR
MFMA	MUNICIPAL FINANCE MANAGEMENT ACT
ACT	MUNICIPAL FINANCE MANAGEMENT ACT (ACT 56 OF 2003) AS AMENDED
ICT	INFORMATION COMMUNICATION TECHNOLOGY
IS	INFORMATION SYSTEMS

### Acronym Description

## 2. INTRODUCTION

The server room is one of the most important physical places in an organisation. The business operations of the municipality depend on the technological systems in the server room, namely servers, switches, UPS's etc. This policy will provide guidelines on controlling the physical server room access.

## 3. POLICY STATEMENT

This policy will help & assist EMLM Corporate Services Department/ICT unit to define the appropriate standards, procedures, and restrictions for the Municipality's server room (s) including:

- **Employee access**
- **Visitor access**
- **Conduct in the server room**
- **Monitoring and audit process**

## 4. PURPOSE

- 4.1 The purpose of this policy is to define standards, procedures, and restrictions for accessing EMLM's internal server room(s).
- 4.2 The overriding goal of this policy is to reduce operating risks. The EMLM Server Room Access Policy will:
  - **Regulate human traffic into the facility which tends to open up security vulnerabilities or cause server outages.**
  - **Protect corporate data, networks, and databases from unauthorized use and/or malicious attack.**



4.3 Therefore, all access to server rooms owned and/or operated by EMLM must be controlled, monitored and conducted in a manner that adheres to EMLM defined processes for doing so.

4.4 This policy is complementary to any previously implemented policies dealing specifically with security and network access to EMLM network.

## **5. RELATED POLICIES, PROCESSES AND PROCEDURES**

This policy shall be read together with all other EMLM ICT policies.

## **6. SCOPE**

This policy applies to all EMLM-OWNED, EMLM-operated, or EMLM-controlled servers and server rooms. The designation or creation of new server rooms within corporate facilities will be managed at the sole discretion of the ICT department. Unapproved access, or use of server rooms, is strictly prohibited.

## **7. POLICY APPLICATION**

This policy applies to all personnel that access the municipality building for performing any work for or with the municipality but not limited to employees, contractors, service providers etc.

## **8. ROLES AND RESPONSIBILITY**

- 8.1 The Senior Manager Corporate Services and ICT Manager of EMLM has the only delegation to approve physical access to any of EMLM's server room (s).
- 8.2 The Systems Administrator of EMLM has the overall responsibility for the confidentiality, integrity, and availability of municipal and information data.
- 8.3 Other ICT staff under the direction of the ICT Manager, are responsible for following the procedures and policies.
- 8.4 All EMLM employees have the responsibility to act in accordance with company policies and procedures.

## **9. PROCEDURE**

It is the responsibility of any employee of EMLM who is accessing the server room to protect EMLM's technology-based resources (such as municipal and information data, computer systems, networks or databases) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Based on this, the following rules must be observed:



## **9.1 LEVELS OF ACCESS**

- 9.1.1 Authorized access: The server room is physically secured by a biometric access controlled door. Additionally: An access register is placed inside the server room to be filled & signed by persons accessing the server room. A listing of currently authorized staff can be found in section Server Room Access List.
- 9.1.2 All staff members included in Server Room Access List have been authorized for access based on job/business related needs. The need for authorization will be reviewed quarterly. 9.1.3 Entry into the server room by "tailgating" other staff is strictly prohibited.
- 9.1.4 Staff must report all security or health and safety incidents to the ICT Manager immediately.
- 9.1.5 ICT Staff is expected to challenge any unescorted visitors within the server room.

## **9.2 VENDOR ACCESS**

- 9.2.1 Vendor must apply in writing to the Senior Manager Corporate Services and ICT Manager for physical access to EMLM Server Room (s).
- 9.2.2 Vendors with approved access to the server room are required to identify themselves to the Systems Administrator and sign in/out of the server room using the Access Register.
- 9.2.3 Vendors are expected to report any security or health and safety incidents to the Systems Administrator immediately.

## **9.3 VISITOR / GUEST ACCESS**

- 9.3.1 In general, casual visits or tours to the server room are not allowed. However, approval of a tour or casual visit may be granted, Requests for a visit or tour to the server room should be directed to the Senior Manager Corporate Services and ICT Manager of EMLM.
- 9.3.2 While on site visitors must be escorted at all times.
- 9.3.3 All visitors will be made aware of this policy. It is the responsibility of the ICT staff member accompanying the visitor to ensure their conduct conforms to this policy.

## 9.4 CONDUCT IN THE SERVER ROOM

In order to maintain a safe and secure environment, it is mandatory for all persons working within and visiting the server room to adhere to the following rules:

- 9.4.1 Cameras are not permitted and taking photographs is strictly forbidden.
- 9.4.2 The use of mobile phones, pagers or other equipment that emit radio waves within the server room is forbidden unless approved by the Systems Administrator.
- 9.4.3 No food or beverages is allowed within the server room.
- 9.4.4 Smoking within the server room is strictly forbidden.
- 9.4.5 No Hazardous materials are allowed within the server room.
- 9.4.6 No cleaning supplies are allowed within the server room without prior approval from the Systems Administrator or ICT Manager.
- 9.4.7 No cutting, grinding, or whittling of any material (pipes, floor tiles, etc) can be performed inside the server room unless special arrangements have been made.
- 9.4.8 All packing material (cardboard, paper, plastic, wood styrene, etc, must be removed from equipment in the staging area before being moved into the server room.
- 9.4.9 All persons are expected to report any security or health and safety incidents to the Systems Administrator immediately.
- 9.4.10 No person shall connect any equipment, network/wireless devices, or monitoring tools without permission or specific Change Control authorization.

## 9.5 MONITORING AND AUDIT

The server room access is controlled and monitored by various sub-systems (Biometric Access Control and Access Register) which produce access records. All server room access records are subject to the following rules:

- 9.5.1 Access records will be monitored by the Information Security Officer, unauthorized access and access which is inconsistent with ICT staff schedules will be investigated and appropriate action taken.
- 9.5.2 Biometric Access Control logs and Access Register will be kept for one year.

MR

M.D



## 9.6 SERVER ROOM ACCESS LIST

The staff listed below is currently authorized for access based on job/business related need. The need for authorization will be reviewed annually. The list below will be reviewed and changed as the ICT staff is being employed.

Title/Position	Department	Access Level	Server Room (s)	Reason
ICT Manager	ICT	24 x 7	All	ICT
Systems Administrator	ICT	24 x 7	All	ICT
Network Administrator	ICT	24 x 7	All	ICT
Information Security Officer	ICT	24 x 7	All	ICT

## **10. COMPLIANCE**

- 10.1.1 All employees and contractors of the municipality are required to comply with this Server Room Access Policy. Non-compliance issues will be handled by the ICT department to ensure that cases of negligence relating to information loss are dealt with accordingly. Each non-compliance case must be dealt with according to the seriousness of the transgression.
- 10.1.2 Any employee found to have violated this policy may be subjected to disciplinary action up to and including termination of employment. Any contractor and or service provider found to have violated this policy may be subjected to having his contract with EMLM terminated and legal action will be taken according to the extent of the offence.

## **11. ADMINISTRATION OF THE POLICY**

This policy shall be administered and enforced by the ICT Manager.

## **12. POLICY IMPLEMENTATION**

- 12.1. Policy implementation will be done by the ICT department.
- 12.2. Any revision to the policy implementation strategy will be approved by the ICT Manager & Director Corporate Services;
- 12.3. The Systems Administrator will ensure that the revised implementation strategy is implemented and subsequent reviews are conducted to review its effectiveness.

## **13. UPDATING THE POLICY**

No amendments are to be made to any section of this policy without such amendment(s) first being: Consulted upon with the ICT Manager of EMLM, AND duly approved and signed by the Director Corporate Services.

## **14. POLICY REVIEW**

This Policy shall be reviewed as and when necessary.


## **15. EFFECTIVE DATE**

The Policy shall be effective once approved by the municipal council.

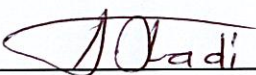


Elias Motsoaledi Local Municipality Server Room Access Policy

16.SIGNATORIES

  
Ms. NR Makgata Pr Tech Eng  
Municipal Manager

30/08/2024  
Date

  
The Mayor  
Cllr. Tladi DM

30/08/2024  
Date