ELIAS MOTSOALEDI LOCAL MUNICIPALITY-MASEPALA WA SELEGAE

A RE BELEGANENG

CLEAN DESK AND CLEAR SCREEN POLICY			
VERSION	**COUNCIL RESOLUTION NO**	**APPROVED DATE**	**IMPLEMENTATION DATE**
01			

MR

M·D

NO	TABLE OF CONTENTS	PAGE NO

MR

M·D

1. DEFINITIONS

1.1. **EMLM** – Elias Motsoaledi Local Municipality.

1.2. **MFMA** – Municipal Finance Management Act.

1.3. **POPIA** - Protection of Personal Information Act, No. 4 of 2013.

1.4. **Compliance** – adhering to the requirements of legislation and organisational standards and codes, principles of good governance and accepted community and ethical standards.

1.5. **Compliance culture** – the values, ethics and beliefs that exist throughout EMLM and interact with EMLM `s structures and control systems to produce norms that are conducive to compliance outcomes.

1.6. **Compliance Management Framework** – a mechanism through which EMLM can monitor, review and comply with legislation, regulations, statutes, codes, standards, policies and procedures.

1.7. **Compliance breach or failure** – an act or omission whereby EMLM has not met its compliance obligations, processes or behavioural obligations.

1.8. **Senior Management or Management** - EMLM staff at a management level who are normally managing different departments and are responsible for the facilitation, monitoring, coordination and communication to EMLM staff their departments on compliance matters.

1.9. **Obligations** – legislation, regulations, statutes, codes, policies, procedures and service standards to which EMLM must comply.

2. POLICY PURPOSE

MR

M.D

2.1. The purpose of this policy is to ensure that all information is adequately protected when unattended. This is best achieved by completely clearing work surfaces of all removable items, where practicable. Work surfaces include, but are not limited to desks, credenzas, tops of cabinets, conference room tables, display boards, and walls. EMLM's goal is to reduce the risks of unauthorized access, loss, and damage to information.

2.2. Information assets can be in any form, ranging from paper documents, sticky notes, or digital forms such as data stored on computers. The mandate of this policy is to ensure that unattended work areas, whether in the EMLM's offices or alternate work site, are clear of information whether in digital or physical form.

2.3. Incomplete and inconsistent clean desk and clear screen controls may lead to unauthorized exposure of sensitive data through unprotected paper trails and computer screens.

3. POLICY SCOPE

3.1 This policy applies to all users as well as third parties who have access to the EMLM's records, documents, agreements, e-mail, internet access or ICT network. The policy therefore applies to all staff members of the EMLM and covers all records regardless of format, medium or age, all third parties who manage the EMLM's information in any manner, all offices and locations of the EMLM, and records at all stages of their life cycle, whether at rest, in transit, or in use.

3.2 Records covered by this policy relates to all recorded information in all formats used in relation to all aspects of the business of the EMLM. Electronic records have the same status as paper records. Both electronic and paper records are bound by the same legislative requirements and are subject to the same degree of confidentiality and care.

4. RELATED LEGISLATIONS AND POLICIES

The following policies and legislations impact on, or are impacted by this policy:

HR

M·D

a. POPIA Compliance Policy Framework

b. Information Classification Policy

c. Information Security Policy

d. Records Management Policy

e. Human Resources Policies

f. Protection of Personal Information Act (POPIA), No. 4 of 2013

g. Promotion of Access to Information Act (PAIA), No. 2 of 2000

5. CLEAN DESK

5.1 All information must be removed from the desk and locked in appropriate containers, drawers, or filing cabinets when the desk is unoccupied and at the end of the workday. This is also applicable when remote working.

5.2 While the EMLM's employee is at the desk, paper documents containing confidential information must be shielded from the view of others who do not have permission to access the information.

5.3 File cabinets must be closed and locked when not in use or when not attended.

5.4 Keys or combinations used for access to information must not be left at an unattended desk, under keyboards, inside pencil cups, in unlocked desk drawers or other areas accessible to anyone.

5.5 Paper and EMLM permitted removable computer media containing confidential information must be stored in secured, lockable storage places, when such media is not in direct control of an authorized individual.

5.6 Information such as passwords, authorization codes, or financial information must not be kept under keyboards, attached to computers, retained on sticky notes, or put up on notice or pin up boards.

5.7 All information written on white boards must be erased immediately after the meeting is over.

5.8 Mobile devices must be password protected and stored in appropriate places.

6. ROLES AND RESPONSIBILITIES

6.1. Employees

This policy is to be adhered to when an employee is away from their workstation for any length of time (momentarily, for a few minutes, or to have a meal or to take a coffee break).

    a. It is employees' responsibility to ensure that the availability, confidentiality, and integrity of information that is entrusted to their custody is not compromised through access by unauthorized persons.

    b. The EMLM's employees need to access data for defined business reasons. It is the employees' obligation to ensure that information is accessed and used only to complete the assigned functions.

    c. All employees are expected to provide the confidential of information for which they are responsible. Although not all inclusive, the following items are some examples of what must not be posted in a public or open area:

        i.   Passwords

        ii.   Contracts

        iii.   Account numbers

        iv.   Intellectual property

        v.   Employee records

        vi.   Medical information

        vii.   Financial information

        viii.   Data on business performance

        ix.   Personal information

        x.   Special personal information

6.2. Managers

Supervisors and Managers are responsible for:

a. Ensuring that their team members clearly understand and follow this policy.

b. Ensuring that appropriate resources (e.g., locking file cabinets) are available for team members to comply with this policy in the workplace, whether in the EMLM's office or when working remotely.

c. Enhancing awareness about this policy through regular communications, reviews, and update sessions.

d. Monitoring on a regular basis compliance with this policy and, where required, reinforcing the message of compliance.

7. CLEAR SCREEN

7.1 Computer workstations and terminals must be locked when unattended. This is also applicable when remote working.

7.2 Computer screens (whether desktop or laptop) must be positioned in a manner that unauthorized persons might not easily view information on the system. If this is not possible or practical, use of a monitor privacy screen is required.

7.3 Computer workstations must be logged off completely at the end of the workday.

8. CONFERENCE TOOLS AND MEETINGS

8.1. Before beginning a new meeting, all information relating to the previous meeting must be cleared and removed from view.

8.2. On finishing a meeting, ensure that the conference room is scrubbed clean of all information and notes, messages, minutes of meetings, agenda items, etc., are not left behind on the desks, the screen, or the white board. If a conference room is to be used exclusively by specific team over multiple days and removal of information is not practical, the room must be locked and made accessible only to authorized employees.

8.3. Confidential Information must not be discussed in public, exposed to public view, or left unattended.

9. PRINTERS AND SHREDING MACHINES

9.1. Confidential information must not be discussed in public, exposed to public view, or left unattended.

9.2. Take printed documents out of the workplace only, if necessary, especially if they contain confidential information.

9.3. Confidential information, when printed, must be immediately cleared from printers.

9.4. Prior to sending documents containing confidential information, verify that the intended recipient(s) of the documents will be individuals permitted to receive such confidential information.

9.5. Confidential information must immediately be cleared from printers and shredding machines areas.

10. DOCUMENTAL DISPOSAL

Documents must be destroyed in a manner that is compliant with the EMLM's Records Management Policy.

11. THIRD PARTY RESTRICTIONS

11.1 Third parties, including family members, must be restricted from the use of home office equipment and personal computers for EMLM's business.

11.2 Repairs of computers used for the EMLM's business must be performed by EMLM's Information Technology (IT) Unit or an EMLM's approved vendor.

12. DEVIATION

There should be no deviation from this policy, any deviation of this policy will be treated as misconduct and dealt with in accordance with the relevant provision of employment of EMLM and where applicable, disciplinary actions will be accordingly taken.

13. IMPLEMENTATION, MONITORING AND EVALUATION

Municipal Management and Line Managers are responsible for the implementation of the policy. The Deputy Information Officers should ensure there is effective monitoring of this policy.
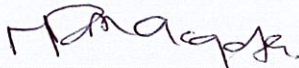
14. REVIEW OF CLEAN DESK AND CLEAR SCREEN POLICY

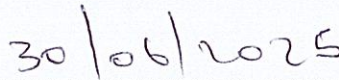This Policy shall be reviewed as and when required.

15. IMPLEMENTATION OF THE CLEAN DESK AND CLEAR SCREEN POLICY

Implementation of this Clean Desk and Clear Screen Policy will take effect from the day approval by council.
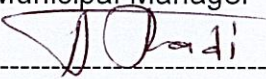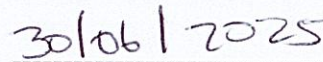
16. APPROVAL

Ms. NR Makgata Pr Tech Eng
Municipal Manager

Mayor
Cllr. MD Tladi

----
30 |06| 2025
Date

--The
30|06| 2025
Date