MARULENG LOCAL MUNICIPALITY

DOCUMENT SECURITY

POLICY

DOCUMENT APPROVAL

Resolution NO :	**SCO5/05 /2023**
Date approved :	**29 / 05 / 2023**
Effective Date :	**01 / 07 / 2023**

Signature _____

VERSION 1 OF JULY 2022

DOCUMENT SECURITY POLICY

1. INTRODUCTION

1.1 This policy, in relationship with all other records management policies and procedures apply to all records created or received by Maruleng Local Municipality in transaction if it's proper business or in pursuance of its legal obligations.

1.2 For the purposes of this policy, records shall be defined as information in any form or medium needed to conduct the affairs of the Maruleng Local Municipality or which need to be maintained or stored for some period of time because of governmental regulation or generally accepted standards. These formats include but are not limited to paper, photographs, film, audio and videotapes, microforms, drawings, databases, email, and other electronic records.

1.3 All such records are the property of Maruleng Local Municipality and are subject to the following designated security classification:

Public: information that can be shared with anyone without damage to the Municipality
Confidential: includes sensitive information which is locked in the strong room

2. SCOPE OF THE POLICY

2.1 Records management underpins an organization through ensuring access to accurate, up-to-date records when required by those that require them. Efficient records management processes will ensure ease of access to information, efficient use of physical

and virtual storage space, legal compliance and reduced duplication of information and effort.

2.2 This policy applies to all records created, received or maintained by the staff of Maruleng Local Municipality in the course of carrying out their corporate functions. Records may be created, received or maintained in hard copy or electronically and act as evidence of a business transaction of Maruleng Local Municipality.

3. ACCESS AND SECURITY

3.1 Records shall at all times be protected against unauthorized access and tampering to protect their authenticity and reliability as evidence of the business of Maruleng Local Municipality.

3.2 Security classified records shall be managed in terms of the Information Security Policy which is attached to this policy and is also available from the Divisional Senior Admin.

3.3 No staff member shall remove records that are not available in the public domain from the premises of Maruleng Local Municipality without the explicit permission of the Senior Admin.

3.4 No staff member shall provide information and records that are not in the public domain to the public without consulting the Senior Admin. Specific guidelines regarding requests for information are contained in the Promotion of Access to information Policy which is maintained by the Senior Admin.

3.5 Personal information shall be managed in terms of the Promotion of Access to Information Act until such time that specific protection of privacy legislation is enacted.

3.6 No staff member shall disclose personal information of any member of staff or client of Maruleng Local Municipality to any member of the public without consulting the Senior Admin first.

3.7 An audit trail shall be logged of all attempts to alter/edit electronic records and their metadata.

3.8 Records storage areas shall at all times be protected against unauthorized access. The following shall apply:

3.8.1 Registry and other records storage areas shall be locked when not in use.

3.8.2 “No Entrance” sign will be displayed at the door and window of the registry Offices

3.8.3 The security gates of the registry offices and other records storage areas shall be Locked at all times when in use as to control access to the registry offices. No unauthorized person (any person that have no direct line functional responsibility inside the registry) must be allowed inside.

3.8.4 Access to server room and storage areas for electronic records media shall be Managed with a key of the office issued to the IT Officer and the spare key locked in the strong room

4. LEGAL ADMISSIBILITY AND EVIDENTIAL WEIGHT

4.1 The records of Maruleng Local Municipality shall at all times contain reliable evidence of business operations. The following shall apply:

4.1.1 **Paper based records**:

4.1.1.1 No records shall be removed from paper-based files without the explicit permission of the records manager.

4.1.1.2 Records that were placed on files shall not be altered in any way.

4.1.1.3 No alterations of any kind shall be made to records other than correspondence files without the explicit permission of the records manager.

4.1.1.4 Should evidence be obtained of tampering with records, the staff member involved shall be subject to disciplinary action.

5. **IMPLEMENTATION**:

A dedicated Records Management Service is already in place and will lead on the implementation of this policy. The policy will be regularly reviewed to keep up to date with rapidly changing technology, business needs and regulatory requirements.

6. **DEFINITIONS**:

Authentic Records:

Authentic records are records that can be proven to be what they purport to be. They are also records that are considered by the creators to be their official record.

Correspondence system:

A set of paper-based and electronic communications and associated documents, sent, received, Generated, processed and stored during the conduct of business.

Electronic records:

Information which is generated electronically and stored by means of computer technology. Electronic records can consist of an electronic correspondence system and electronic record systems other than the correspondence system.

Public record:

A record created or received by a governmental body in pursuance of its activities, regardless of form or medium.

Records other than correspondence systems:

Records that do not form part of a correspondence file, or a case file e.g. registers, maps, plans, electronic records, audio-visual records, etc.

Record:

Recorded information regardless of form or medium.
Evidence of a transaction, preserved for the evidential information it contains.

Schedule for records other than correspondence systems:

A control mechanism for records other than correspondence files (other records), which contains a description and the disposal instructions and retention periods of all other records. It consists of the following parts:

- Schedule for paper-based records other than correspondence files;
- Schedule for electronic records systems other than the electronic correspondence system;
- Schedule for microfilm records;
- Schedule for audio-visual records.

7. **REFERENCES**:

National Archives and Records Service: Records Management Policy Manual, April 2006
National Archives and Records Service: Managing electronic records in governmental bodies: Policy, principles and requirements, April 2006
National Intelligence Agency: Minimum Information Security Standard (MISS).