
ELIAS MOTSOLEDI LOCAL MUNICIPALITY-MASEPALA WA SELEGAE



INFORMATION CLASSIFICATION POLICY

VERSION	COUNCIL RESOLUTION NO	APPROVED DATE	IMPLEMENTATION DATE
01			

NO	TABLE OF CONTENTS	PAGE NO
1	DEFINITIONS	3
2	POLICY OBJECTIVE	5
3	PURPOSE	5
4	POLICY STATEMENT	6
5	APPLICABILITY	6
6	ROLES AND RESPONSIBILITIES	6
7	RELATED DOCUMENTS AND POLICIES	7
8	USER RESPONSIBILITY	8
9	ACCESS CONTROL	8
10	CLASSIFICATIONS LABELS	10
11	LABELING	11
12	THIRD -PARTY INTERACTIONS	13
13	HANDLING INFORMATION	14
14	HANDLING CONFIDENTIAL INFORMATION	14
15	DISPOSAL	16
16	DEVIATION	16
17	REMEDIAL ACTION	17
18	REVIEW OF INFORMATION CLASSIFICATION POLICY	17
19	IMPLEMENTATION OF THE INFORMATION CLASSIFICATION POLICY FRAMEWORK	17
20	APPROVAL	17

MR

M.D

1. DEFINITIONS

- 1.1 **MM** - Municipal Manager
- 1.2 **EMLM** - Elias Motsoaledi Local Municipality
- 1.3 **PAIA** - Promotion of Access to Information Act, No 2 of 2000
- 1.4 **POPIA** - Protection of Personal Information Act, No. 4 of 2013
- 1.5 **Archives** - Records no longer in active use containing permanent historical information of EMLM, the term is used to describe the physical site where records of permanent (enduring) value are arranged, described, preserved and made available.
- 1.6 **Active record** - Refers to a record needed for daily administrative and/or operational functions from the date of creation until no longer needed to be frequently retrieved, up to a maximum of two years old, that is kept in the office of origin.
- 1.7 **Authenticity** - An authentic record is one that can be proven to be what it purports to be, have been created or sent by the agent purported to have created or sent it and have been created or sent at the date and time purported.
- 1.8 **Authoritative records** - Records, which, regardless of form or structure, possess the characteristics of authenticity, reliability, integrity and usability. The authoritativeness of records is supported by their being managed by records systems that are reliable, secure, compliant, comprehensive and systematic. (ISO 15489 – Records Management)
- 1.9 **Correspondence records** - Paper-based and electronic communications and associated documents, sent, received, generated, processed and stored during the conduct of business.
- 1.10 **Destruction** - Refers to the disposal of documents of no further value by deletion, shredding, pulping, etc.
- 1.11 **Disposal** - Refers to the actions taken about records as a consequence of the expiration of their retention periods. Disposal is not synonymous with destruction. Disposal may involve one of the

following activities: Transfer to a storage facility or records centre, Transfer of permanent records to archives; or Destruction of ephemeral records.

- 1.12 **Document** - Refers to paper, electronic forms and files, emails, faxes, contracts, leases, vendor communications, etc. which are still editable.
- 1.13 **Electronic record** - Information which is generated electronically and stored by means of computer technology. Electronic records include records which are converted from paper to electronic through the process of scanning.
- 1.14 **Filing system** - Is the collective noun for a storage system (like files, boxes, shelves or electronic applications and storage systems) in which records are stored in a systematic manner and a method for storing and organising computer files and the data they contain to make it easy to find and access them. File systems use a data storage device such as a hard disk, on-line storage repository or CD-ROM and involve maintaining the physical location of the files.
- 1.15 **Classification** - The act or process by which information is determined to be sensitive or non-sensitive information.
- 1.16 **Sensitive information** - Information that, as determined by EMLM, must be protected because its unauthorized disclosure, alteration, loss or destruction will at least cause perceivable damage to EMLM, including its employees, service providers or other stakeholders.
- 1.17 **Folder** - Is an organised arrangement of records on the same subject accumulated in chronological order within the same cover/ container. A container could be a logical grouping of related electronic files in the electronic system.
- 1.18 **Personal information** - Means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person in terms of the POPIA.
- 1.19 **Record** - Refers to recorded information, regardless of format or medium (i.e., paper and electronic, including e-mails and other records), which has been created, received, used, accessed and maintained by EMLM (and/or its predecessors) which should be retained as evidence and in

pursuance of its legal obligations or in the transaction of business. Included are e-mails, records in electronic form and records other than correspondence.

1.20 **Retention** - Refers to the process of deciding which records to keep permanently and which records to be destroyed after they no longer serve a useful purpose. Retention periods are documented in this policy.

1.21 **Special personal information** - Special Personal Information in terms of the POPIA.

1.22 **Usability** - The ability for a record to be located, retrieved, presented and interpreted.

1.23 **Records manager** - The employee delegated to oversee the records management within EMLM and who is responsible for compiling guidance for best practice records management and for promoting compliance with the organisation's Records Management Policy.

2. POLICY OBJECTIVE

The objective of this policy is to give effect to sensitivity classification requirements of EMLM's information and to ensure that EMLM information is:

- 2.1. Classified in terms of its value, legal requirements, sensitivity, and criticality to the organisation; and
- 2.2. Available to those who need it, and is used, transferred, stored and ultimately disposed of in accordance with the classification.

3. PURPOSE

The intention of this policy is to define sensitivity classification, ensure that it is applied to all information in the EMLM, and that information is protected and managed accordingly. The purpose of this policy is to:

- 3.1. Establish the framework needed for effective sensitivity classification of information;
- 3.2. To provide mandatory stipulations on the classification, labelling, handling and use of EMLM's classified information.
- 3.3. Ensure that EMLM protects classified information according to its level of classification; and

- 3.4. Ensure that EMLM classifies and protects information containing personally identifiable information in accordance with applicable privacy laws.

4. POLICY STATEMENT

All information created and received by EMLM shall be managed in accordance with applicable legislation, including the POPIA, the PAIA, and the International Standard for Information Security Management (ISO 27001). Information must be classified in terms of its value, legal requirements, sensitivity, and criticality to EMLM. All the EMLM's information must be stored in approved storage systems and locations.

5. APPLICABILITY

5.1. This policy impacts upon EMLM's work practices for all those who:

- 5.1.1. Create information.
- 5.1.2. Have access to information.
- 5.1.3. Have any other responsibilities for information, for example capture, storage and maintenance responsibilities; and
- 5.1.4. Have management responsibility for staff engaged in any these activities; or manage, or have design input into, information technology infrastructure.

5.2. The policy therefore applies to all staff members of EMLM, all third parties who manage EMLM's information in any manner and covers all information regardless of format, medium or age and applies to information at rest, in transit, or in use.

5.3. The information covered by this policy relates to all recorded information in all formats used in relation to all aspects of the business of EMLM. This policy is applicable to all offices and locations of EMLM and includes any third-party locations where EMLM's information is stored or managed.

6. ROLES AND RESPONSIBILITIES

6.1. The Information Officer

The Municipal Manager is the Information Officer. The Information Officer in terms of PAIA and POPIA is ultimately accountable for the information sensitivity classification practices within EMLM. The

Information Officer may formally delegate duties and responsibilities to Deputy Information Officer or various officials within EMLM to perform operational information sensitivity classification functions.

6.2. Departmental Senior Managers

Departmental Senior Managers are responsible for the implementation of this policy in their respective business units and ensuring that all staff are made aware of and are trained and equipped to perform their information sensitivity classification responsibilities and obligations.

6.3. The Records Manager

The operational responsibility for information sensitivity classification rests with the Records Manager as the custodian of this Information Classification Policy.

6.4. The IT Unit

The IT Unit has the following responsibilities:

- (a) Provision and maintenance of information sensitivity classification functionality within EMLM's ICT systems.
- (b) Ensure the confidentiality, integrity and availability of digital information in any approved EMLM's ICT System, including but not limited to e-mail systems, network drives or transactional systems; and
- (c) Ensure that access controls in ICT systems support the classification requirements.

6.5. Employees

All employees must comply with this policy and must follow authorised procedures in carrying out information sensitivity classification functions, and must observe security, privacy, and confidentiality requirements at all times, in accordance with this policy and Information Security Policy.

7. RELATED DOCUMENTS AND POLICIES

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

- 7.1. Records Management Policy
- 7.2. Information Security Policy
- 7.3. Human Resources Policies
- 7.4. POPIA Compliance Policy Framework

8. USERS AND RESPONSIBILITIES

This policy is applicable to all information in the possession of or under the control of EMLM. Every user is personally responsible for the protection of information that has been entrusted to their care. All users who come into contact with confidential internal information are expected to familiarize themselves with this Information Classification Policy and to consistently use these same ideas in their daily business activities.

9. ACCESS CONTROL

9.1. NEED TO KNOW

- (a) EMLM's information sensitivity classification system, as defined in this policy, is based on the well-known concept called "need to know." This term means that information must not be disclosed to any person who does not have a legitimate business need for the information. This fundamental concept, when combined with all of EMLM's subject-specific policies, assists in protecting confidential information and information classified as for "Internal Use Only" in paragraph 11.3 from unauthorised disclosure, use, modification and deletion.
- (b) This policy assists in optimizing designated security by allowing EMLM to determine what security measures are required for sensitive information that requires protection and where it is located.

9.2. DECISION TO GRANT ACCESS

- (a) Decisions to grant access to information must be subject to the provisions laid down in the PAIA and conditions of POPIA if access relates to personal information and/or special personal information. All information containing "Personal Information" and/or "Special personal information" as per the POPIA shall be labelled "Highly Confidential" and managed according to EMLM's POPIA Compliance Policy Framework to personal information and/or special personal information, access can only be granted after the approval of the Information Officer – Municipal Manager, after an assessment has been conducted by the Deputy Information Officer of the legitimacy of the request.
- (b) Background verification checks on all candidates for employment, contractors, and third-party users shall be carried out in accordance with relevant laws, regulations, and ethics, and

5/12

M.D

proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

9.3. ACCESS BY INTERNAL STAFF

- (a) Access to EMLM's IT systems will be granted only through the approval of the user's line manager or supervisor.
- (b) EMLM's IT systems privileges to users shall be promptly terminated at the time when a user ceases to provide services to the EMLM. The data of individuals who leave the organisation will be kept on the server for a minimum of 90 days. If no directive with regards to the re-use of the information is received from the said user's component or supervisor, the data shall be removed from the server and be archived in the form of a backup.
- (c) EMLM management reserves the right to revoke the privileges of any user at any time if it is found that the user's conduct adversely interferes with the normal and proper operation of the EMLM IT systems, or if such conduct is harmful or offensive to others.
- (d) Physical access to IT resources shall be granted in accordance with formally defined procedures. Only authorized personnel shall have physical access to IT equipment.

9.4. THIRD PARTY ACCESS

- (a) Third parties maybe given access privileges to the IT resources after the IT Manager has determined that they have legitimate business needs upon receiving a written request from the line manager or head of the department under which the said third party will be working. These privileges shall be enabled only for the time period required to accomplish approved tasks and this access will not be allowed from a remote location.
- (b) Third party access shall be monitored and reviewed on regular basis.
- (c) Any third party who requires access to the IT resources of EMLM shall, before such access is granted, sign a non-disclosure agreement to protect the confidentiality of systems and information they access.
- (d) A third party shall provide any information reasonably necessary for the EMLM to evaluate security issues relating to any authorized third party's employee.
- (e) The third party shall notify the EMLM in writing immediately upon a change in the user base.

9.5. VISITORS ACCESS

- (a) No visitors shall be allowed access to any of the IT resources of the EMLM or to the server rooms unless they obtain approval from the IT manager, except for internet access via the Guest Access Point through the Wi-Fi. The hosting party/person shall be responsible for ensuring that required approval is obtained before any access is granted.
- (b) Where access to the server rooms is granted by the IT Manager, the visitor shall not enter a server room unless accompanied by the hosting staff member and monitored by responsible staff member.

10. CLASSIFICATIONS LABELS

There are four classification labels, which are as follows:

10.1.HIGHLY CONFIDENTIAL

Sensitive information considered as Highly Confidential is not to be shared beyond those who need to know. The unauthorised disclosure, alteration or destruction of that information could significantly adversely impact EMLM or its data subjects such as service providers or employees. The highest level of security must be applied to Highly Confidential information. The following are examples of Highly Confidential information:

- (a) Personal Information in terms of POPIA
- (b) Special Personal Information in terms of POPIA;
- (c) Information that could compromise EMLM's operations, patents, or intellectual property; and
- (d) Committee meeting packs and related information flows.

10.2.CONFIDENTIAL

This classification label applies to information that is intended for use within EMLM. Its unauthorised disclosure could adversely impact on EMLM or its data subjects such as service providers or employees. Information that some people would consider to be private is included in this classification. Examples include employee performance evaluations, computer passwords, and internal audit reports.

10.3.INTERNAL USE ONLY

This classification label applies to information that does not clearly fit into classification "Highly Confidential" Or "Confidential" but is not suitable for public disclosure. While its unauthorised disclosure

is against policy, it is not expected to impact on EMLM seriously or adversely, or its data subjects such as employees and service providers. Examples include EMLM's new employee training materials and internal policies and procedures.

10.4.PUBLIC

This classification applies to all other information, not deemed to be confidential or for internal use only. By definition, there is no such thing as unauthorised disclosure of this information, and it can be disseminated without potential harm. Examples include advertisements, job announcements, and information that has been approved for release to the public.

11. LABELING

All information must be labelled. Information without a label is by default classified as "Internal Use Only". If information is confidential, it must be labelled "Confidential" from the time it is created until the time it is destroyed or transferred. This label must appear on all manifestations of the information, such as on paper copies, floppy disks, and CD-ROMS, digital copies and storage media such as Flash drives, CDs, DVDs, magnetic tapes, etc. Users are not allowed to remove or change classification labels for confidential information unless the written permission of the information originator has been obtained.

11.1.INCORRECT LABELLING

If the recipient of internal information believes that the data classification label accompanying this information is incorrect, the recipient must protect the information in a manner consistent with the more stringent of the four possible classification labels. Before using this information or distributing it to any other party, such a recipient must check with the information originator to ensure that the label currently applied to the information is correct.

11.2.STORAGE MEDIA

Information with different levels of sensitivity classification (highly confidential, confidential, internal use or public information) must not be stored, for current use or future storage, in a single folder (paper or electronic) or on a single removable storage device (e.g. CD, DVD, USB flash drives, or any technological storage devices that may be developed in future).

MR
M.D

11.3. LABELS FOR THIRD PARTY INFORMATION

With the exception of general business correspondence and copyrighted software, all external third-party information (it is personal information of third parties) that is not in the public domain must receive a sensitivity classification system label of 'confidential'. The employee who receives this information is responsible for assigning an appropriate classification on behalf of the third party. When assigning a classification label, the employee must preserve copyright notices, author credits, guidelines for interpretation and information about restricted dissemination.

11.4. LABELLING PAPER-BASED RECORDS

All printed, handwritten, or other paper manifestations of confidential information must have a clearly noticeable sensitivity label on the upper right-hand corner of each page. If bound, all paper manifestations of confidential information must have an appropriate sensitivity label on the front cover, the title page, and the back cover.

The cover sheet for documents containing confidential information must contain the appropriate classification label. Microfiche and microfilm, video and sound cassettes also must contain labels if they contain confidential information. When applied, sensitivity labels must not cover, overlay or obscure any information in the document.

11.5. LABELLING REMOVABLE ELECTRONIC STORAGE MEDIA

All CD-ROMs, DVD's, magnetic tapes and other removable electronic storage media that contain highly confidential or confidential information must be labelled externally with the appropriate sensitivity classification. Computer files containing highly confidential or confidential information must clearly indicate the relevant classification label in the first two data lines.

11.6. OTHER DISPLAYS

If information is highly confidential or confidential, all instances in which it is displayed on a screen or otherwise presented to a user must involve an indication of the information's sensitivity classification. Teleconferences and telephone conference calls where highly confidential or confidential information must be discussed must be preceded by:

- (a) A statement by the convener of the conference about the sensitivity of the information involved.

112

M.D

- (b) A determination by the convener of the conference that all parties to the discussion are authorised to receive highly confidential or confidential information.
- (c) Persons other than those specifically invited by the convener of the meeting must not attend meetings where confidential information must be discussed.

11.7.PUBLIC INFORMATION LABELS

Unless it is unquestionably already public information, all information with a public label must also be labelled "Approved for Public Release" along with the date when the originator declared the information public.

11.8.CHANGES TO LABELS

Information sensitivity may change over time. For example, intellectual property may be confidential whilst a new product is being developed. Once that product is in daily use the sensitivity may change to internal use only or public access. At that time, a formal process must be followed to document the authority, date and purpose for such change, and the information re-labelled accordingly.

12. THIRD-PARTY INTERACTIONS

12.1.THIRD PARTIES AND THE NEED TO KNOW

Unless it has been specifically designated as "public", all internal information must be protected from disclosure to third parties. Third parties may be given access to internal information only when a demonstrable need to know exists, and when such a disclosure has been expressly authorised by the relevant information originator. Contractors, consultants, temporary employees, volunteers, and every other type of individual or entity that is not an employee, is by definition a third party for purposes of this policy.

12.2.DISCLOSURES TO THIRD PARTIES AND NON-DISCLOSURE AGREEMENTS

The disclosure of highly confidential or confidential information to consultants, contractors, temporary employees or any other third parties must be preceded by the receipt of a signed non-disclosure agreement. Disclosures of highly confidential or confidential information to these third parties must be accompanied by a written running log indicating exactly what information was provided. This log is important when the time arrives to recover these materials or obtain a letter certifying destruction of the materials at the end of a contract.

12.3.INFORMATION ORIGINATOR NOTIFICATION

If confidential information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the information originator and the Records Manager must be notified immediately

13. HANDLING INFORMATION

All users must observe the requirements for handling information based on its sensitivity classification. Information originators may designate additional controls to further restrict access to, or to further protect their information. Extra security measures should be applied to records containing information classified by POPIA as special personal information.

14. HANDLING CONFIDENTIAL INFORMATION

14.1.MAKING COPIES

Making additional photocopies or printing extra copies of highly confidential or confidential information must not take place without the prior written permission of the information originator.

14.2.UNATTENDED PRINTING

Printers must not be left unattended if highly confidential or confidential information is being printed or must be printed. Unattended printing of highly confidential or confidential information is permitted only if physical access controls are used to prevent unauthorised persons from entering the area by the printer and viewing the material being printed

14.3.PAGE NUMBERING

All confidential information manifested in paper form must indicate both the current and the total number of pages, for example, "Page 2 of 9."

14.4.BACKUP STORAGE MEDIA

All highly confidential or confidential information recorded on backup computer media and stored outside EMLM offices must be controlled by access control measures.

MR
M.D

14.5.ENVELOPES

Envelopes containing highly confidential or confidential information must be addressed to a specific person and must contain sufficient return address information. All highly confidential or confidential information sent through these delivery systems must require a signature by an authorised party at the destination.

If highly confidential or confidential information is to be sent through internal mail, it must be delivered by hand with a control register which must be signed by the recipient.

14.6.REMOVAL FROM OFFICES

Any classified information removed from EMLM premises must comply with the Information Security Policy. Highly confidential or confidential information must not be removed from EMLM premises unless there has been prior written approval from the delegated authority. This policy includes all storage devices, and hard-copy output. An exception is made for authorised offsite backups. The Records Manager and Municipal Manager authorise such backups.

EMLM has the right to confiscate devices if they have a suspicion that the employee they belong to must not have access to the information contained on them; for example, classified data.

The IT Unit has the authority to manage EMLM information on both EMLM -owned and user-owned devices. When an employee leaves the employment of EMLM all relevant documentation and EMLM devices containing such information is handed over to EMLM as part of the exit procedure.

14.7.TRANSMITTING CLASSIFIED INFORMATION

Confidential information must be transmitted by secure means only

14.8.LOCKED CONTAINERS IN THE OFFICE

When not in active use, highly confidential or confidential information in paper-based form must be locked in offices, safes, heavy furniture or other facilities or containers approved by the Records Manager. Unattended highly confidential or confidential information found lying on a desk after business hours, or highly confidential or confidential information that is otherwise readily accessible to passers-by after hours, may be confiscated and later claimed in person from the Records Manager.

14.9.LOCKED CONTAINERS OFF-SITE

Whenever a paper-based version of highly confidential or confidential information contained on removable media, is removed from EMLM premises, it must be properly locked away. All reasonable precaution has to be taken to ensure that confidential information cannot be accessed by unauthorised persons. Such information must not be left in an unattended motor vehicle, hotel room, office, or some other location, even if the vehicle or room is locked.

14.10. ORAL WARNINGS

If confidential information is released orally in a meeting, or related presentation, the speaker must communicate the sensitivity of the information. The speaker must remind the audience not to disclose this information to others. Visual aids such as presentation materials, projector slides and overhead transparencies must include the appropriate data classification labels.

15. PHYSICAL SECURITY

15.1.OFFICE ACCESS

Access to every office, computer room, and work area containing highly confidential or confidential information must physically restricted. Management responsible for the employees working in these areas consults the relevant authority to determine the appropriate access control method.

15.2.LOCKED WHEN NOT IN USE

Confidential information must be protected from unauthorised disclosure when not in use. When left in an unattended room, such information must be locked appropriately.

15.3.UNAUTHORISED SCREEN VIEWING

The screens of computers used to reflect confidential information must be positioned in such a way that unauthorised viewing is impossible.

16. 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.

MR

M.D

17. REMEDIAL ACTION

Any breach/violation of this compliance policy is considered serious and remedial action would be instituted, and proper sanctions will be effected (upon guilty verdict/ if found guilty)

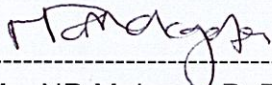
18. REVIEW OF INFORMATION CLASSIFICATION POLICY

This Policy shall be reviewed as and when required.

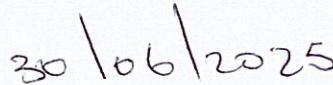
19. IMPLEMENTATION OF THE INFORMATION CLASSIFICATION POLICY

Implementation of this Information Classification Policy will take effect from the day approval by council.

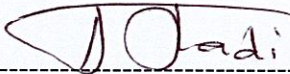
20. APPROVAL



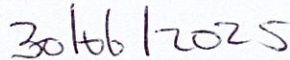
Ms. NR Makgata Pr Tech Eng
Municipal Manager



Date



The Mayor
Cllr. MD Tladi



Date