ELIAS MOTSOALEDI LOCAL MUNICIPALITY-MASEPALA WA SELEGAE

INFORMATION SECURITY POLICY

MUNICIPAL COUNCIL RESOLUTION NUMBER

M24/25-07

APROVED AT THE 4TH ORDINARY COUNCIL SITTING OF 30 AUGUST 2024

Table of Contents

M.D MR

1. Definitions

Term	Meaning
IT	Information Technology
Information Technology	Information Technology (IT) is a broad subject for managing and processing information.
Information Technology Steering Committee (IT STECO)	is a committee of senior management that directs, reviews, and approves IT strategic plans, oversees major initiatives, and allocates resources.
Password	A secret series of characters which when used together with a USERID enables a user to access a file, computer, or program. Each Elias Motsoaledi Local Municipality workstation user must enter his or her password before the computer will respond to commands. The password helps ensure that unauthorized users do not access the computer. In addition, data files and programs may require a password.
User ID	The User ID is a unique identification of Elias Motsoaledi Local Municipality workstation users. The User ID is used to gain access to Information Technology systems. User IDs are also used to audit workstation user's activities.
IT Security	Refers to techniques for ensuring that data stored on an Elias Motsoaledi Local Municipality workstation or server cannot be read without authorization or compromised in any way. Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.
Administrative rights	Access rights that allow a user to perform high-level/administrative tasks on a device/application such as adding users, deleting log files, and deleting users.
Biometric information	Personal information obtained through biometric measurements, such as fingerprints, retina, DNA, etc.
Internal system processes	Processes that are performed by the system with no human intervention. Part of the internal working of the system or application.
Information Security	Includes, but is not limited to the protection of information against unauthorized disclosure, transfer, loss, modification, and destruction, whether accidental, environmental, or other adversarial threats.
Users	Elias Motsoaledi Local Municipality's employees and other workers including consultants and contractors.
Information	Any electronically generated data as well as written documents, which pertain to Elias Motsoaledi Local Municipality's financial, technical, operational, governance, and related records.
Information classification	The assignment of specific named levels of classification is defined within Elias Motsoaledi Local Municipality's Information Classification Policy. Such an assignment is being used to identify value, significance, and necessary protective measures.
Information resources	Includes, but is not limited to the following: • The procedures, equipment, facilities, software, and data that are

M.D

Term	Meaning
	designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information. Employees are also a very important information resource. • Data networks, servers, personal computers, and mobile computing devices (Including all Elias Motsoaledi Local Municipality-owned or managed, or any other device that contains Elias Motsoaledi Local Municipality-owned information), all end-user devices connected to the Elias Motsoaledi Local Municipality's networks, such as storage media, printers, photocopiers, fax machines, supporting equipment, and back-up media, as well as computer login codes.
Data Subjects	Individual employees, service providers, community members, council members, external members of governance structures, and other stakeholders of whom the Municipality processes their personal information.

2. Introduction

The Municipality has seen an increase in interest in the topic of information security. This is primarily motivated by the strategic value of data and/or information, which acts as proof of prevailing socioeconomic problems and provides the framework for service delivery solutions. In addition to the issues, the surge in cybercrimes and the need to comply with regulations highlight the significance of implementing sufficient safeguards to safeguard municipality-owned information.

Information Security concerns itself with tools and processes an organization, a Municipality, in this case, employs to protect its information. The main objective of information security is to ensure that the information possessed remains confidential, adheres to the highest standards of integrity, and most importantly accessible to those who have authority to use it. For this policy, we consider information security in the context of Information and Communication Technologies (ICT).

In addition, this policy aims to guide procedures related to data collection, processing, deletion, and/or loss, as well as how relevant parties should be informed.

3. Legislative Frameworks

The policy was drafted bearing in mind the legislative conditions and other Municipal policies, as well as to leverage nationally recognized ICT standards.
The following legislation, among others, was considered in the drafting of this policy.

- Constitution of the Republic of South Africa, Act No. 108 of 1996.
- Copyright Act, Act No. 98 of 1978.
- Electronic Communications and Transactions Act, Act No. 25 of 2002.
- Minimum Information Security Standards, as approved by Cabinet in 1996.
- Municipal Finance Management Act, Act No. 56 of 2003.
- Municipal Structures Act, Act No. 117 of 1998.
- Municipal Systems Act, Act No. 32, of 2000.
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996.

MR

M.D

- National Archives Regulations and Guidance.
- Promotion of Access to Information Act, Act (PAIA) No. 2 of 2000.
- Protection of Personal Information Act (POPIA), Act No. 4 of 2013.
- Regulation of Interception of Communications Act, Act No. 70 of 2002.
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following nationally recognised ICT standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014
- Control Objectives for Information Technology (COBIT) 5, 2012
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- King Code of Governance Principles, 2016

The following Municipality's policies must also be read with this policy:

- POPIA Compliance Policy Framework
- Records Management Policy
- Information Classification Policy

4. Purpose

The policy's purpose is to offer direction on what steps the municipality will take to stop or lessen acts that could jeopardize the integrity of the entire municipality by attacking its infrastructure, information, and ICT systems maliciously. Additionally, to guarantee that the right technologies are used to increase the protection of the institution's information, this policy aims to define the acceptable use of ICT resources by Officials and any party providing services to or on behalf of the Municipality. This policy also outlines the Municipal Manager and Management's commitment to the protection of the Municipality's information resources. The policy shall assist:

4.1. The Municipality to effectively identify, manage, measure, and monitor potential information security risk exposures ensuring that all information assets are protected against all internal, external, deliberate, malicious, environmental, or accidental threats.

4.2. With the establishment of an effective structure to govern Information Security for the Municipality.

4.3. In outlining roles and responsibilities of stakeholders in information security management.

This policy defines the general rules for using business information received or generated by the Municipality or its staff and the systems and equipment that store and process that information. It also provides general guidance on the protection of personal privacy of the Municipality's Data Subjects such as employees, service providers, community members, and other stakeholders.

MR

M.D

By implementing appropriate security measures, the Municipality will be able to support its decisions with reliable data as it works to accomplish its goals and objectives, thereby improving the lives of regular residents.

5. Scope

The policy applies to everyone in the Municipality, including its 3rd party service providers and consultants. This policy is regarded as being critical to the security of the ICT systems of the Municipality.

The policy covers the following elements of information security:

- Ownership and classification of information.
- Security incident management.
- Physical security.
- Application security.
- Network security.
- Change control; and
- Software authorization and licensing.

Procedures will apply to electronic information systems that maintain Information Technology to assure that such systems are accessed only by those persons or software programs that have been granted access rights.

6. Breach of policy

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. The appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services.
- Disciplinary action by the Municipal policy; or
- Civil or criminal penalties, e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
- Punitive recourse against a service provider in terms of the contract.

7. Administration of the policy

The System Administrator and ICT Manager or delegated authority is responsible for maintaining the policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and any changes approved by the Council.

8. Protection of Classified Information

8.1. Council members, officials, including 3rd party service providers and consultants are required to exercise a strict degree of self-discipline to prevent the

MR

M.D

communication of sensitive or classified information by the Municipal Systems Act, Act No. 32 of 2000, Schedule 1: Code of Conduct for Councillors and Schedule 2: Code of Conduct for Municipal Staff Members. Officials and council members are not permitted to give unauthorized individuals access to any privileged or secret information.

8.2. All municipal data must be classified in compliance with the 1996 Cabinet-approved Minimum Information Security Standards and terms of the classification labels described in the Information Classification Policy.
8.3. Access to classified information is determined either by the level of security clearance or if the information is required in the execution of their duties.
8.4. Officials, in conjunction with the ICT Manager, must ensure that classified information receives adequate protection to prevent compromise.
8.5. Officials who generate sensitive information are responsible for determining the information classification levels. This responsibility includes the labeling of classified documents.
8.6 When a government post is being appointed, a declaration of secrecy must be issued on an official form, according to Section 1 of Chapter 6 of the Minimum Information Security Standards.

9. Protection of Personal Information

9.1. Personal information is defined as any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person in terms of the POPIA No. 4 of 2013. Elias Motsoaledi Local Municipality is required by law to comply with any relevant data protection/privacy legislation when obtaining, storing, or processing personal information.
9.2. Employees have a personal responsibility to comply with this policy and relevant international and national privacy legislation. Failure to comply with privacy legislation is a criminal offence and individuals can be held personally liable for breaches. Employees should contact their line manager if they have any questions relating to privacy legislation compliance.
9.3. The Bill of Rights in the Constitution states that the public has a right to privacy, as well as a right to access personal information held by the Municipality.
9.4. The PAIA gives effect to the right to access personal information held by the Municipality and must be complied with.
9.5. The POPIA gives effect to the right to privacy. The Act requires that the Information Officer of the Municipality ensure that personal information is lawfully obtained and processed.
9.6. The ICT Manager and Officials must work together to ensure the following concerning personal information (only key points of the Act included):
   a) Identify the systems and locations where personal information can be found.
   b) Ensure that Municipal policies, in particular those that deal with information security, are applied to the systems and locations where personal information is collected, processed, and disposed of;

c) Put in place business process controls to ensure that personal information is collected lawfully, is complete and accurate, and updated where necessary.
d) Dispose of excessive personal information, after consultation with the Records Manager.
e) Put in place structures and systems to allow the access of persons to their personal information stored by the Municipality. The requester may request to have their personal information deleted or corrected if it is incorrect or obtained unlawfully; and
f) Ensure that systems do not use personal information as the sole basis to decide legal consequences for a person or group of persons (referred to as "automated decision making").

9.7. POPIA Section 6, contains certain general exceptions where the Act does not apply e.g. the processing of personal information for national security, defense, public safety, law enforcement, or for the judicial functions of a court.

9.8. POPIA prohibits the processing of certain categories of special personal information. The general exception is where a competent person (e.g. in the case of children) has given consent, or if an exception applies.

9.9. The following personal information is not regarded as special personal information and must be protected in terms of the general rules for the protection of personal information: Gender, sex, marital status, age, culture, language, birth, education, financial, employment history, identifying number, symbol, e-mail address, physical address, telephone number, location, online identifier, personal opinions, views, preferences, private correspondence, views or opinions about a person, or the name of the person if the name appears next to other personal information or if the name itself would reveal personal information about the person.

9.10. The PAIA prohibits the disclosure of certain types of information held by the Municipality, including, but not limited to personal information. These include:

- Commercial information of a third party.
- Information that falls under a confidentiality agreement.
- Information that is likely to endanger the safety of individuals if it is made public.
- Police dockets in bail proceedings.
- Records privileged from production in legal proceedings.
- Research information of a third party.
- Security information about a building, structure, or system.
- Methods, techniques, procedures, or guidelines for law enforcement and legal proceedings.
- Information that will prejudice the defense, security, and international relations of the Republic.
- Information that will jeopardize the economic interests and financial welfare of the Republic and the commercial activities of the Municipality.
- Research information of the Municipality; and
- Information about the operations of the Municipality.

9.11. PAIA requires that information relating to public safety, environmental risk, or a substantial contravention of, or failure to comply with the law, be disclosed immediately.

MR

M.D

10. Handling of confidential information

10.1. All users must observe the requirements for handling information based on its sensitivity classification described in the Information Classification Policy. 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.

10.2. Employees are responsible for ensuring that confidentiality is not compromised while sensitive files and/or documents are in their possession. Employees must:

10.2.1 Ensure that any sensitive paper-based information is appropriately secured whenever they leave their desk unattended.

10.2.2 Make use of the screen locking facilities when they leave their computer unattended for extended periods.

10.2.3 Ensure that when logging on, passwords are not made visible to anyone and always log in at the end of the day.

10.2.4 Manage the risks associated with the use of laptops, removable media, and external storage devices (e.g., USB drives) by taking care of their possession and encrypting any sensitive business data where possible.

10.2.5 Take precautions and care with IT equipment such as laptops and information when working in a public place.

11. Conditions for Elias Motsoaledi Local Municipality Access Control

GENERAL CONTROL ENVIRONMENT

11.1. To ensure the reliability of ICT services and to comply with legislation, all Municipal systems and infrastructure must be protected with physical and logical security measures to prevent unauthorized access to Municipal data.

11.2. Physical and logical security is a layered approach that extends to user access, application security, physical security, database security, operating system security, and network security.

11.3. Employees, who request User Access Accounts for network or physical access must -

- Agree to respect all relevant policies and procedures on electronic data processing security and the confidential nature of the information obtained.
- Occupy a position in which access to information contained on the municipal servers and/or premises is considered necessary or useful.
- Have the approval of their immediate superior or the head of the department/section in which they work and of the IT Unit.
- Server Room Access register must be filled and signed by both the IT officer allowing access to a visitor and the time entering & exiting the server room must be stated.
- Desktops & Laptops must automatically lock themselves after 5 minutes to avoid intrusion without the knowledge of the user.

M.D

- Long cables to key lock laptops with a pin code or access code must be provided to laptop holders and the ICT unit will depend on physical security to guard desktops.
- An employee who is not logged on to our system for 30 consecutive days, his/ her account shall be disabled automatically for security purposes and be activated as soon as the employee logs a call.

12. Physical Security

12.1 A maintenance schedule must be created and maintained for all ICT hardware under the control of the ICT department. Maintenance activities must be recorded in a maintenance register.

12.2 Officials of the Municipality must be made aware of the acceptable use of ICT hardware.

12.3 All hardware owned by the Municipality must be returned by employees and service providers when no longer needed or on termination of their contract.

12.4 All data and software on hardware must be erased before disposal or reuse. The removal of the data from the computers and laptops, which include records containing the personal information of the Municipality's data subjects, by the ICT Unit must be done in a manner that the data cannot be reconstructed into its intelligible form as prescribed by section 14(5) of POPIA.

12.5 Any hardware that carries data that can be carried off-site (e.g. laptop computers, removable hard disks, flash drives, etc.) must be protected with encryption.

12.6 ICT hardware and software must be standardized as far as possible to promote fast, reliable, and cost-effective ICT service delivery to the Municipality.

Access Control Procedures

13. Access Request

13.1. Users must complete the required access request form to gain access to the Municipality network. This form -

13.1.1. Identifies the applicant as an employee of Elias Motsoaledi Local Municipality

13.1.2. Specifies the type of information needed in connection with the applicant's duties.

13.1.3. Provides the applicant's undertaking to observe all pertinent policies and procedures.

13.1.4. Provides a record of approval of the applicant's superiors.

13.2. Requests may be initiated either by the employee or by the employee's supervisor, but both must sign the access request form.

13.3. The form is to be sent to the IT Security officer for approval. Authorization of access request forms must be done as per delegation by management.

MR

M.D

14. Unique User Identification and Password

14.1. Elias Motsoaledi Local Municipality users will have a unique login ID/ username. Users who no longer have access shall have their login IDs suspended or deleted promptly.

14.2. Login IDs with root or supervisor access need to be extremely safe. Users with these credentials are not permitted to use these IDs for regular, daily work; instead, they must be kept for system management activities.

14.3. Electronic access is controlled through authentication. Each user will be uniquely identified and passwords will be used to authenticate identity. The network operating system shall be configured to encourage a periodic expiration of all passwords as well as to establish a suitable minimum length for passwords.

14.4. Each user's password must meet the following conditions –

14.4.1. Passwords must be a minimum of eight or more characters in length. Administrative, system, and other privileged accounts should employ a password of eight or more characters in length:

14.4.2. Passwords must incorporate three of the following characteristics -

Any lower-case letters (a-z)
Any upper-case letters (A-Z)
Any numbers (0-9)
Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @%^ & * ( ) _ - + = { } [ ]:; " ' | \ / ? < > , . ~ `)

14.4.3. Passwords must not be words found in a dictionary.

14.4.4. Passwords must not include easily guessed information such as personal information, names, user IDs, pets, birth dates, etc.

14.5. If a system does not support the minimum structure and complexity as detailed in the guidelines, one of the following procedures must be implemented –

13.5.1. The password assigned must be adequately complex to ensure that it is not easily guessed, and the complexity of the chosen alternative must be defined and documented.

14.6. Users must not allow another user to use their unique user identification or password.

14.7. Users must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner.

14.8. Users are responsible and accountable for access under their identifiers.

14.9. All files containing protected Elias Motsoaledi Local Municipality information shall be stored on the network, with the appropriate access controls.

14.10. Access rights and privileges for all authorized users shall be maintained and managed to secure access to data in a manner appropriate to the needs of the user and the value of the data.

MR

M.D

14.11. Each user must ensure that their assigned User Identification is appropriately protected and only used for legitimate access to networks, systems, or applications. If a user believes their user identification has been comprised, they must report that security incident to the appropriate ICT Unit and IT Security Officer.

15. Passwords Policy

15.1. A computer access password is the primary key to computer security. The importance of password maintenance and security cannot be over-emphasized.

15.2. All employees/users of the municipality's computer facilities are solely responsible for the integrity and secrecy surrounding passwords allocated for their usage.

15.3. The password uniquely identifies employees/users and allows access to the municipality's information and computer services. For employees/user's protection, and the protection of the municipality's resources, employees/users must keep their password secret and not share it with anyone else.

15.4. The username shall be the first character of a user's first name & surname e.g. tseroto for Thabo Seroto

15.5. Users create their password on their computers and the ICT Office has the right to reset, or over-write once the user has forgotten or requested it to be changed.

16. Passwordrds Policy Statements

16.1. All user-chosen passwords for computers and networks shall be difficult to guess.

16.2. Construct fixed passwords by combining a set of a minimum of eight alphanumeric characters.

16.3. It is forbidden for users to generate passwords that exactly match or closely resemble ones that have already been used.

16.4. Passwords shall not be stored in readable form in batch files, automatic login scripts, software macros, or terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them.

16.5. All vendor-supplied default passwords shall be changed before any computer or communications system is used.

16.6. All passwords shall be changed immediately if they are suspected of being disclosed or known to have been disclosed to unauthorized parties.

16.7. Regardless of the circumstances, passwords shall never be shared or revealed to anyone else by the authorized user.

16.8. Users are responsible for all activity performed with their user IDs and therefore are not allowed to share their user IDs with anyone else.

16.9 Systems Passwords will be set to automatically change every 30 days.

16.10. At most, five minutes of idleness will trigger Windows screen savers.

MR

M·D

16.11. Should users forget their password, they must contact the ICT Unit for assistance.

17. Password Attempt

17.1. A user's account will automatically block and then automatically unblock after 30 minutes if they fail to enter their password correctly 3(three) times. Alternatively, they can contact the ICT department to have their account unblocked. Password attempts are limited to three (3) attempts.

18. Automatic Logoff

18.1. Servers, workstations, or other computer systems containing information that has been classified as high risk must employ inactivity timers or automatic logoff mechanisms. The systems must terminate a user session after a maximum of 5 minutes of inactivity.

18.2. Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit, receive, or store information must employ inactivity timers or automatic logoff mechanisms.

18.3. Applications and databases using medium or high-risk ratings, such as medical records, must employ inactivity timers or automatic session logoff mechanisms.

18.4. If a system that otherwise would require the user of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented -

18.4.1. The system must be upgraded or moved to support the required inactivity timer or automatic logoff mechanism.

18.4.2. The system must be moved into a secure environment.

18.5. When leaving a server, workstation, or other computer system unattended, the user must lock or activate the system's automatic logoff mechanism (e.g. CNRL, ALT, DELETE, and Lock Computer) or logout of all applications and database systems containing information.

19. Use of Elias Motsoaledi Local Municipality Access Accounts

19.1. Access accounts may be used only for the purpose for which they were issued. Any use for private purposes is prohibited. Employees are responsible for the security of their password and all use of their access account. Accounts that remain inactive for prolonged periods may be suspended/ disabled without warning or notice. A written or oral request to reinstate the access shall be addressed to the IT Security Officer.

19.2. Abuse or negligence in handling the access account will result in the withdrawal of access privileges, cancellation of the account, and appropriate disciplinary measures.

19.3. System and Network access accounts will be renewed periodically if the incumbent occupies the position for which the account was issued and continues to need the same access privileges. If different access privileges

HR

M.D

become necessary, or if the user is transferring to another position within the Elias Motsoaledi Local Municipality, a new access request must be submitted.

20. Virtual Private Network Access (VPN)

20.1. The Network Controller shall ensure that all networks that contain Elias Motsoaledi Local Municipality systems and applications are appropriately secured -

20.1.1. Dialup connections directly into secure networks are considered to be secure connections and do not require a VPN connection. This implementation of secure remote access extends the secure network to the remote user using a secure PSTN (Public Switched Telephone Network) connection.

20.1.2. Authentication and encryption mechanisms are required for all remote access sessions to networks containing Elias Motsoaledi Local Municipality information via an ISP (Internet service provider).

20.2. The following security measures must be implemented for any remote access connection into a secure network containing Elias Motsoaledi Local Municipality information -

20.2.1. Use of technology to bypass authorized remote access mechanisms (e.g. VPN) is strictly prohibited. For example, the use of remote-control software and applications such as PC Anywhere, GoToMyPC.com, and Team Viewer to bypass VPN access mechanisms is NOT permitted without prior written consent from the ICT Manager.

20.2.2. Remote access systems must employ a mechanism to "clear out" cache and other session information upon termination of the session.

20.2.3. Remote access workstations must employ a virus detection and protection mechanism.

20.2.4. Users of remote workstations must comply with Elias Motsoaledi Local Municipality Security Policy.

21. Unauthorized Access Rights

21.1. A username is to be suspended/disabled immediately (or appropriate measures be taken to address the matter) when the individual user no longer needs access to the computer system or terminates employment with the municipality.

21.2. If users change work positions, their access rights will be reviewed and changed to match their new job description. Management may restrict or extend computing privileges and access to their information resources. The ICT Unit must be notified by the head of the department, human resource unit, or the supervisor of the official concerned to suspend the user account.

22. Protection against Unauthorized Access

22.1. It is the responsibility of the Information and Communication Technology Unit to ensure that Elias Motsoaledi Local Municipality systems and data are safe

M.D

and secure from unauthorized access that might lead to alteration, damage, or destruction of automated resources and data, unintended release of data, and denial of service.

22.2. It is the responsibility of every user to ensure that the information and data on their computer are stored in a safe place and according to standards, circulars, and policies stipulated by Elias Motsoaledi Local Municipality and its ICT Unit.

23. Movement of Hardware

23.1. Any movement of computer hardware between the Elias Motsoaledi Local Municipal buildings as well as off the premises is restricted and controlled by the ICT and Asset Management Unit.

23.2. A further critical consideration is the security of any information contained in it. Often, the data and information are more valuable than the equipment itself.

23.3. When a user or employee moves ICT equipment, they must obtain approval from the Asset Management unit, the ICT Manager, and their respective Head of Department. Movement resulting from office relocations must also be notified to the ICT Unit.

24. Orientation

24.1 The Information Technology Unit will hold orientation sessions for the newly employed personnel before a password is given to the user. The training session will among other things include network login, e-mail and internet access, printing, file sharing, etc.

24.2. Additionally, one-on-one training or group training can be scheduled if there are drastic changes in the system especially those that need thorough communication with the user(s).

E-Mail Control Procedures

25. Email Security

a) The ICT Manager must make all users aware of the safe and responsible use of e-mail and Internet services. E-mail and Internet should only be used for official use. Personal usage can be permitted if it does not interfere with job functions. E-mail and the Internet may not be used for any illegal or offensive activities.

b) Officials and the ICT department may not use Internet cloud services (e.g. Google Drive, Gmail, Dropbox, etc.) for official purposes unless approved by the ICT Steering Committee.

25.1 Risk of Emails

25.1.1 Since e-mail includes both the transmission and handling of sometimes-sensitive information, care must be taken to protect the message from unauthorized access. Threats can include the ability of individuals to change and copy information, or to distribute information to unauthorized parties.

MR

M.D

Users can also act anonymously, or with a fake identity, and spread information under assumed names.

25.1.2 The use of e-mail is therefore open to several commercial risks, including -

25.1.2.1. Accidental change or distribution of messages through error or negligence
25.1.2.2. Unauthorized use, processing, or distribution of messages
25.1.2.3. Distortion, interruption, or unwanted disclosure of messages
25.1.2.4. Unauthorized disclosure of confidential, proprietary, or trade secret information

25.2 E-Mail Naming Standards

25.2.1. The following naming standards have been agreed to and will apply to all Elias Motsoaledi Local Municipality e-mail users –

25.2.1.1 The first initial of the user and surname of the user will be used as the e-mail identification.
25.2.1.2. When defining a new username and/or e-mail identification, if such a name already exists, the second initial will be utilized.
25.3.1.3. No nicknames will be used as network or e-mail identification.

25.3 Size Limits of Mailboxes and E-mail Attachments

25.3.1 The following limits will apply and be adhered to by all EMLM e-mail users –

25.3.1.1. A size limit of 100 GB per mailbox.
25.3.1.2. A size limit of 25MB for Sending and receiving mail, inclusive of original message plus attachments.
25.3.1.3. If an e-mail attachment exceeds 25MB the user needs to compress the files to be attached in such a way that it does not exceed 25MB.

25.4 E-Mail Policy Statements

25.4.1 Private use is permitted but this is subject to strict control. Abuse of this privilege may be regarded as misconduct.
25.4.2. From time to time the use of the Email system may be audited.
25.4.3. The Municipality reserves the right to inspect the e-mail at any time without notice.
25.4.4. Through using e-mail, you will have been deemed to have read, understood, and agreed to the policies relating to e-mail systems contained within these documents.
25.4.5. Users should never give proprietary, trade secret, or sensitive information to outside parties. After reading, dispose of any extraneous emails received from the email system. All critical email attachments need to be kept in the workstation's My Documents folder for future reference and regular backups.

M.D

25.4.6. Users should exercise caution when opening email attachments to check for viruses, especially if the attachment contains an executable application. If users open a message and are prompted to "Enable or Disable macros" users should select "Disable". If a user has any suspicions about an email they have received, they should contact the ICT Unit.

25.4.7. If users get an attachment via e-mail, that is unsolicited, or of unknown origin, detach it and scan the file using the installed antivirus software. Alternatively, delete it.

25.4.8. Avoid unnecessarily large distribution lists.

25.4.9. Ensure that the content of the message cannot be misinterpreted and that there is nothing unlawful about the transmission or content of the message.

25.4.10. From time to time, certain disclaimers may be required for messages requiring confidentiality, legal privilege, etc. Please request assistance from the Municipal Legal Officer.

25.4.11. It is prohibited to forward or transmit: Offensive, defamatory, discriminatory, or harassing material, sexually explicit or other offensive images, Unlicensed copyright material, non-business-related video, and image files, confidential, proprietary, or trade secret information outside without authorization, advertisements, and chain letters.

25.4.12. Users are prohibited from sending or forwarding e-mail notices concerning virus or harmful code warnings to other employees and "broadcast" e-mail messages unnecessarily.

25.4.13. When using electronic mail to communicate with users on the Internet -

25.4.13.1. Do not automatically forward internal mail to an Internet site.

25.4.13.2. Do not use autoreply functions to respond to your Internet mail.

25.4.13.3. When using the autoreply to functions such as the Out of Office message option for normal municipality's internal mail, be sure to select the option that excludes sending the notices to Internet users.

25.4.14. Users shall not use an electronic mail account assigned to another individual to either send or receive messages.

25.4.15. Users should regularly move important information from electronic mail message files to word processing documents, databases, and other files, as e-mail messages may be erased periodically, either accidentally or as part of normal archiving and file maintenance functions.

25.4.16. If users receive unwanted and unsolicited e-mail (also known as SPAM), they shall refrain from responding directly to the sender. Instead, they should contact the ICT Unit.

25.4.17. It is the responsibility of individual users to manage their e-mail accounts, users are advised to delete unwanted e-mails and important attachments should be saved in an appropriate folder within the "My Documents" folder of the workstation and saved to a network server for backup. Users can contact the ICT Unit should further information regarding the management of e-mail be required.

25.4.18. Only municipal employees, council members with active employee numbers, and ICT-approved service providers are permitted to access email.

25.4.19. Every outgoing message should contain a disclaimer at the end e.g.

M.D

"1. All views expressed herein are the views of the author and do not reflect the views of the Municipality unless specifically stated otherwise.
2. The information is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material.
3. If you have received this message in error, please notify the sender, from which this message emanates, immediately.
4. Any unauthorized use, alteration, or dissemination is prohibited.
5. Please note that Elias Motsoaledi Local Municipality and all its branches only bind themselves by way of signed agreements. 'Signed' refers to a hand-written signature, excluding any signature appended by 'electronic communication' as defined in the Electronic Communications and Transactions Act, no. 25 of 2002

Internet Control Procedures

26. Internet Security Policy

a) Municipal information, computing assets, and corporate image on the Internet are critical to our success, and as a result, must be protected from loss, modification, or destruction.

b) The Internet should only be used for official use. Personal usage can be permitted if it does not interfere with job functions. Internet may not be used for any illegal or offensive activities.

26.1. Risks of the Internet

26.1.1. On the Web, one of the real dangers is a possible loss of company privacy or leakage of information about municipal activities. The following issues relate to users' privacy when surfing the web -

26.1.1.1. When users visit a website, the site they are visiting can identify where their Internet connection originates. For example, if users use the Web from work, activities can be identified as coming from the municipality.

26.1.1.2. Websites can log all the users' activity including any personal data they provide. The website owner can associate users with this data on future visits.

26.1.1.3. Some websites do not respect data privacy laws and may make the information collected from you available to other organizations.

26.1.1.4. Viruses are designed at best to cause some discomfort and at worst to cause the alteration and loss of data on a computer. Viruses pose a tremendous threat and can be introduced in several ways, particularly from files and programs downloaded from internet sources and via e-mail attachments. It is therefore imperative that all computers in use have approved anti-virus software loaded and activated to update and scan viruses automatically and regularly. Contact the ICT Unit if you are in any doubt about either a message or file content.

26.2 Internet Security Policy Statements

MD

26.2.1. Employees may only use municipal facilities to access the Internet with permission from department management. Internet access that is granted automatically is not a right, and it can be stopped if it is discovered that the service is being abused.

26.2.2. When an employee writes anything on an electronic bulletin board, Internet discussion group, or other public information system, they must include a disclaimer that states unequivocally that the remarks do not always reflect the opinions of the municipality.

26.2.3. Unless expressly authorized by the Municipal Manager, when using municipal information and/or systems, all employees are forbidden from participating in internet discussion groups, chat rooms, or other public electronic forums except for work-related purposes.

26.2.4. Users shall not advertise, promote, present, or otherwise make statements about municipal products and services in internet forums such as mailing lists, news groups, or chat sessions without the prior approval of the Municipal Manager.

26.2.5. Although the internet is an informal communication environment, the laws for copyrights, patents, trademarks, etc. apply. Employees using Elias Motsoaledi Local Municipality internet or communication systems shall:

26.2.5.1. Resend material only after obtaining permission from the source.

26.2.5.2. Quote material from other sources only if these other sources are identified.

26.2.5.3. Reveal internal municipality's information on the Internet only if the information has been officially approved for public release by the Municipal Communication Section.

26.2.6. When using municipal information systems, or when conducting municipality's business, employees shall not deliberately conceal or misrepresent their identity.

26.2.7. The ICT Unit may prevent users from connecting with certain non-business websites. The ability to connect with a specific website does not in itself imply that employees are permitted to visit that site.

26.2.8. No user or independent contractor to the municipality may use the available Internet, Intranet, or e-mail services provided by the municipality to access newsgroups, Internet websites, and FTP sites for unauthorized and/or unacceptable purposes such as, but not limited to -

26.2.8.1. The viewing and/or downloading of pornographic or obscene material of any nature.

26.2.9. All software and files downloaded from internet sources via the Internet (or any other public network) shall be screened with approved virus detection software before being run or examined via another program such as a word processing package.

26.2.10. All users wishing to establish a connection with the municipality's computers via the Internet shall authenticate themselves at a firewall before gaining access to the municipality's internal network. Contact the ICT Unit for further information.

MR

MD

26.2.11. Non-municipal computers are prohibited from connecting to the municipal networks without specific written permission from the Municipal Manager.

26.2.12. Dial-outs or connections to any non-municipal systems or networks while simultaneously connected to the internal network are prohibited.

26.2.13. Dial-up connections e.g. whilst traveling or from home-based systems and laptop computers which are also utilized for municipal business must only be made via authorized dial-up procedures that employ the use of firewalls and are configured by the ICT Unit.

27. Third Party Access Control
Business agreement

27.1. When the responsibility for the municipality's information processing is outsourced to any external institution or organization, security controls, and procedures shall be addressed in a business agreement between the parties to ensure that the security of the municipality and government information is not compromised.

27.2. In contracting for ICT-related services with external parties, the basic point of departure shall be that an institution shall select only those vendors who undertake to comply with the security measure set in this policy and any other applicable regulation or policy of the Government.

27.1 Business Requirements

27.1.1. The needs of the business process must be addressed by either a manual or computerized system. The business requirements must be clearly defined and documented, otherwise, other issues may take their place, such as the recommendations of the ICT partner or supplier, which has a valid, but separate agenda. In many cases, managers find it seemingly complex to document their needs beyond high-level requirements. However, by recalling the view of Information Security, the high-level requirements may be refined further by specifying the needs of the system concerning

27.1.1.1. Identification and authentication

27.1.1.2. Authorization

27.1.1.3. Confidentiality – who can see/amend what.

27.1.1.4. Integrity – a system that is proven, tested, and has security and fall-back routines in case of need.

27.1.1.5. Availability – the system must be available to users in multiple offices both on workstations and on their laptops.

27.1.1.6. Non-denial

27.1.2. Access control should be established that would limit or detect access to critical resources (e.g. data, files, application programs, and computer-related facilities and hardware), which helps to prevent unauthorized modification, disclosure, loss, or impairment of data.

27.1.3. The ICT Unit shall employ the prevention technique of isolating or segmenting the network with firewalls to block unauthorized incoming traffic, direct incoming traffic, and protect vulnerable systems. Information Technology Unit

M.D

will ensure that Anti-virus software is installed at the network perimeters and deployed to all workstations.

27.2 Basic Security Requirements

27.2.1. Persons responsible for commissioning outsourced computer processing must ensure that the services used are from reputable companies that operate by quality standards which should include a suitable service level agreement that meets the requirements of the Elias Motsoaledi Local Municipality as regulated by the government. The Contractual agreement shall include the following –

27.2.1.1. The legal requirements to be met, for example, data protection legislation.

27.2.1.2. Arrangements to ensure that all parties involved in the outsourcing, including sub-contractors, are aware of their security responsibility.

27.2.1.3. The measures for maintenance and testing of assets to ensure the integrity and confidentiality of institutional business assets.

27.2.1.4. The physical and logical controls to be implemented to restrict and limit access to sensitive business information to unauthorized users.

27.2.1.5. Measures to maintain the availability of services in the event of a disaster.

27.2.1.6. The levels of physical security to be provided for outsourced equipment.

27.2.1.7. The right to conduct a security audit.

27.2.2. All Municipal users must report actual or suspected security breaches or security weaknesses to the Help desk officer or the delegated authority.

27.2.3. The IT Security officer must record all information regarding security incidents. The IT Security officer must review all the information security incidents quarterly to ensure that the root cause of the problems is addressed.

27.2.4. Investigations into security incidents may only be carried out by the IT Security officer or a nominated person.

27.2.5. The Protection of Personal Information Act, Act No. 4 of 2013 prescribes that the Regular and the person affected by the breach must be notified in the event of a breach of personal information.

28. Change Management Control

28.1. All changes to Municipal applications and infrastructure must be managed in a controlled manner to ensure fast and reliable ICT service delivery to the Municipality, without impacting the stability and integrity of the changed environment.

a) Corrections, enhancements, and new capabilities for applications and infrastructure will follow a structured change control process.

b) An emergency change must follow a structured change control process, but with the understanding that documentation must be completed afterward.

MR

M·D

Emergency changes are only reserved for fixing errors in the production environment that cannot wait for more than 48 hours.

c) Recurring change requests from users (e.g. user access requests, a password reset, an installation, move or change of hardware and software, etc.) must follow the processes designed to deliver ICT services most effectively.

d) Recurring operational tasks are excluded from the structured change control process.

29. Roles and Responsibilities

29.1. Policy Owner

The owner of this policy is the Municipal Manager the Information Officer of Elias Motsoaledi Local Municipality, who is accountable and responsible for updates to this policy.

29.2. Management

29.2.1. Management is responsible for identifying risks and the implementation of information security controls throughout the organization, in line with this policy.

29.2.2. Management shall determine the information resources its employees, consultants, partners, and third parties need to access to complete their job functions.

29.3. Deputy Information Officer

The Deputy Information Officer is responsible for facilitating the development, approval, and implementation of this information security policy which prescribes the relevant security measures to be applied.

29.4. Users

Elias Motsoaledi Local Municipality's employees and other workers including consultants and contractors are responsible for:

29.4.1. The Municipality's information assets are used only in the proper pursuit of the Municipality's business following this information security policy.

29.4.2. Ensuring that information is not improperly disclosed, modified, or endangered.

29.4.3. Ensuring that access to the Municipality's information resources is not made available to any unauthorized person.

29.4.4. Reporting information security breaches.

29.4.5. Every employee shall adhere to information security controls applicable to his/ her environment:

29.5. ICT Unit

MR

M.D

29.5.1. The ICT Manager is responsible for the administration of this policy.
29.5.2. The ICT Manager shall be responsible for ensuring that the document remains up to date, practiced, and always enforced.
29.5.3. This policy needs to be acknowledged and understood by all computer users of the municipality and all requests for changes shall be submitted to the Help Desk office in the appropriate format. Please see the form below as an example –

29.6. IT Security Officer Responsibilities

The IT Security Officer is responsible for the administration of this procedure. Responsibilities of the IT Security Officer –

29.6.1. File all the access request forms for record should they be needed later.
29.6.2. Ensure that users are aware of security requirements, procedures, and policies.
29.6.3. Review the user lists to maintain the security databases and tables current.

ELIAS MOTSOALEDI
LOCAL MUNICIPALITY

Job Card No:	JOBCARD
Building name	: Infrastructure /Stores /Main /Commando
User name	: Mokganyetji Moffart
Department	: Strategic department
Departmental unit	: Communications
Telephone Number	: (013) 262 3056
Logged Call date	: 08 December 2014
Area	: Groblersdal/Rossenekal
Name of a IT official Responding	: Katlego / Thabo / Mary / Sibongile / Thabiso
Problem description	: Configuration of new email and IP-Address settings

STATEMENT OF WORK

MR

M.D

Resolution:

User Acceptance	Signature ……	Time Spent ……	How is the Service ……	Date Completed ……/……/20…. Hour……

Job card Approved By IT Official	Name Print ……	Signature ……	Received date by a IT official ……/……/20…… Hour……
Job card Approved By ICT Manager	Name Print ……	Signature ……	Date ……../……../20……

30. Documentation and Procedures

30.1. All change requests shall be documented in the approved format.
30.2. Only approved changes shall be affected.

31. Routine Authorized Maintenance

31.1. Routine maintenance can be affected without necessarily going through the change control process, provided -
311.1. The change impact has been evaluated and is minimal.
31.1.2. There is a known, backout and recovery strategy in case of failure to effect the change.
31.1.3. There are known and tested business continuity strategies that can be affected in the event of failure of the change.

32. Software Release Policy

32.1. Only authorized and licensed software can be released to the ICT environment at Elias Motsoaledi Local Municipality. Distribution or installation of unlicensed software is strictly prohibited.
32.2. Officials may not install or change the software on their computers

33. Distribution of Software

33.1. Software may not be distributed to more users than Elias Motsoaledi Local Municipality is licensed for.

34. Signatories

MR

M.D

Ms. NR Makgata Pr Tech Eng
Municipal Manager

30/08/2024
Date

The Mayor
Cllr. Tladi DM

30/08/2024
Date