



END USER INFORMATION SECURITY POLICY

VERSION 01.15

APPROVED BY:

DATE REVIEW:

POLICY STATEMENTS

GENERAL POLICIES

1. Every employee must familiarise themselves and comply with this and other Langeberg Municipal information security policies.
2. Every employee will execute any particular security process or task assigned to them.
3. All information systems are owned by Langeberg Municipality and users are only permitted to use the facilities for official use.
4. Every employee has a duty to protect the records of the entity, whether it is for regulatory, contractual or operational requirements.
5. Every employee has a duty to report security incidents, weaknesses or non-compliance with the security policies as quickly as possible.
6. It is not permitted to deliberately attempt to breach security systems.

LEGISLATIVE FRAMEWORK

The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognised ICT standards.

The following legislation, among others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, 1996.

Langeberg Municipality holds a large quantity of information that could cause difficulties if it falls into the wrong hands or become inaccessible. Every employee needs to make sure that information is secure from the moment that it is collected or created, whenever it is used, when it is stored and finally, when it is disposed of.

Furthermore, there is a legal duty to keep information secure and to use ICT systems in a secure way. Finally, everyone who uses electronic communications represents Langeberg Municipality and as such must use ICT systems in a responsible manner.

This policy highlights the main duties that every employee needs to know and adhere to. For the purpose of this policy the terms “users” or “every employee” include councillors, contractors and third parties.

Failure to comply with this policy may result in disciplinary action and including dismissal, civil or criminal action, or a combination of both.

- 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
- National Archives Regulations and Guidance
- Promotion of Access to Information Act, Act No. 2 of 2000
- Protection of Personal Information Act, Act No. 4 of 2013
- The Cybercrimes Act 19 of 2020
- Regulation of Interception of Communications Act, Act No. 70 of 2002

ACCESS TO SYSTEMS AND NETWORK

1. Access to information systems and network are forbidden, unless formally authorised.
2. Passwords must be kept secret and must not be shared or store the password in such a way that it can be seen by third parties.
3. Never use obvious passwords such as a birth date or a pet's name.
4. Always select strong passwords i.e. at least 10 characters in length and a combination of alpha-numeric characters, with at least one uppercase / lowercase combination.
5. Passwords must be changed immediately if they are suspected to have been compromised.
6. Passwords may not be stored in any automated log-on process, macro or function key.
7. Systems should be Logged-off if they are not in use or when computers are left unattended, unless the computer has an automatic screen locking mechanism.
8. Never use another employee's account to access systems.
9. The use of multi-factor authentication (MFA) on critical systems should be prohibited where necessary to provide an extra layer of protection making use of additional authentication methods, such as One-Time PINs (OTP), Biometrics, and/or Graphical Passwords (CAPTCHAs).

E-MAIL AND INTERNET

1. Langeberg Municipality monitors electronic communications with the use of electronic communication tools.
2. E-mail and Internet access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or X-rated.
3. Sending of racially or sexually harassing messages/files is also prohibited.
4. No abusive, profane, or offensive language is to be transmitted through Langeberg Municipality's e-mail or Internet system, including any other messaging system.
5. Every staff member has a responsibility to maintain and enhance Langeberg Municipality's public image and to use e-mail and access to the Internet in a responsible manner.
6. Do not participate in chain messages or similar schemes.
7. Solicitation of non-Langeberg Municipality business or any use of Langeberg Municipal e-mail or Internet for personal gain is prohibited.
8. Each employee is responsible for the content of all text, audio or images that they place or send over the organisation's e-mail / Internet system.
9. All messages communicated on Langeberg Municipality's e-mail / Internet system must contain the employee's identity.
10. The official e-mail address or any other form of identification that links the employee to Langeberg Municipality may not be used on social media (e.g. Facebook, news groups, etc.) if the employee does not officially represent an opinion of Langeberg Municipality.
11. Electronic mail forwarding to external e-mail addresses is not permitted.
12. Never save personal data, official passwords or e-mail address on computers, software or public websites.
13. Always be aware of statements in electronic mails that may be viewed by third parties as binding contracts.
14. Employees may not use any free Internet services (e.g. e-mail addresses or data storage) for official use unless previously authorised by the ICT Department as they may not be secure.
15. Employees may not use the Internet to attempt to gain access to computers, files, services etc.

SOFTWARE OR OTHER INFORMATION PRODUCTS

1. Users may not install or change the software on their computers.
2. The IT department may only authorise software from known, reputable sources to reduce the likelihood of introducing errors or security risks into the environment.

COMPUTER VIRUSES

1. Every employee must be aware of the risk of viruses and always follow safe

computing practices, such as:

- Do not use any devices for official use that do not have updated anti-virus software installed.
- Do not interfere with the operation of anti-virus software installed.
- Do not download and launch files or software from external networks, E-mails or removable media unless absolutely necessary for official purposes. If such a need arises, consult with the ICT Department.
- Do not visit websites that are not reputable.
- Take note of warnings and awareness communication from the ICT Department relating to virus and/or phishing alerts.
- In the case of virus detection, discontinue work and report the incident immediately to ICT Department.

MOBILE COMPUTING AND PERSONAL DEVICES (BYOD) EMPLOYEES AND COUNCILLORS

1. No personal owned devices will be allowed on the network of the Municipality.
2. Every Employee will be made aware of the fact that the Langeberg Municipality owns business information on the mobile devices and reserves the right to enforce security measures and to confiscate the device and recover or delete the information remotely without notice.

MOBILE COMPUTING AND PERSONAL DEVICES (BYOD) CONTRACTORS AND THIRD PARTIES

1. The Municipality acknowledges that mobile computing is becoming a common way of working; however, information security risks must be addressed accordingly. Therefore, all methods of mobile computing and personal contractors and third-party devices must be approved by the Manager: ICT preceded by the recommendation of the Network Administrator prior to connecting to the Municipal ICT network, and subjected to a security assessment.

ACCESS TO THE NETWORK

1. Access to the Municipality network may not be established without approval.
2. Remote access to the network may only be used for official and legal purposes.

TRAVELLING OR WORKING FROM HOME

1. Employees' security responsibilities extend outside normal working hours.
2. When travelling or working from home, take due care not to lose or have your equipment stolen.
3. Never leave equipment in public places and always keep your network password confidential.
4. All requirements imposed by insurance policies on equipment security must be complied with.
5. VPN access times is between 07H00 and 23H00.

MEMORY STICKS, PORTABLE HARD DISKS, ETC (REMOVABLE MEDIA)

1. Removable media must be encrypted, or password protected if it is taken off-site and at risk of being lost or stolen.
2. Removable media may not be thrown away but given to the ICT Department to be securely disposed of.

IT EQUIPMENT

1. IT equipment owned by the Langeberg Municipality will be returned to the ICT Department if not in use.
2. Any official information contained on personal equipment must be removed in the event of changing employment.

BACKUPS

1. Save official data/information to the share locations (e.g. H-Drive, T-Drive, OneDrive), which forms part of the backup strategy.
2. Employees are responsible for their own backups if they choose to save official data/information to PCs storage, mobile devices and/or any other removable storage.

PROTECTION OF PERSONAL INFORMATION

1. Personal information may not be collected and stored by anyone unless safeguarded in accordance with legislation.
2. No equipment, information or software may be taken off-site without prior authorisation.

SYSTEMS DEVELOPMENT

1. Employees may not perform any changes to systems, develop new systems, or acquire new package software, outside of the established change control process.
2. The use of desktop applications (e.g. spreadsheets or databases) for a specific purpose is discouraged if it makes better sense to develop a formal system on a server.
3. If an employee chooses to use desktop applications for an important purpose, the following safeguards must be considered:
 - The functionality must be tested.
 - The versions of the desktop application must be managed.
 - Access to the application and its functionality must be appropriately restricted.
 - Access to the file server directory must be restricted.
4. The data must be backed up regularly.

AGREEMENT

I have read this document and acquainted myself with its content. I understand Failure to comply with this policy may result in disciplinary action and including dismissal, civil or criminal action, or a combination of both.

Signed at _____ on this _____ day of _____ 20____.

Employee / Contractor Name and Surname

Manager: ICT

Employee / Contractor Signature