



ICT SECURITY CONTROL POLICY V3.0

2024/2025

ICT Policy No: 4
Revision: Version 3
Last Review: 27 October 2020
Effective From: 1 July 2024
<https://www.laingsburg.gov.za>

ICT SECURITY CONTROLS POLICY

TABLE OF CONTENTS

1. INTRODUCTION	5
2. LEGISLATIVE FRAMEWORK.....	5
3. OBJECTIVE OF THE POLICY	6
4. SCOPE.....	6
5. BREACH OF POLICY	7
6. ADMINISTRATION OF POLICY.....	7
7. PROTECTION OF CLASSIFIED INFORMATION	7
8. PROTECTION OF PUBLIC RECORDS	8
9. PROTECTION OF PERSONAL INFORMATION	9
10. PROTECTION OF RECORDS TO PRESERVE LEGALITY.....	12
11. GENERAL CONTROL ENVIROMENT.....	13
12. PHYSICAL SECURITY	13
13. DATABASE SECURITY	13
14. NETWORK SECURITY.....	14
15. E-MAIL AND INTERNET	15
16. WIRELESS NETWORKS.....	15
17. MOBILE DEVICES AND OWN HARDWARE (BYOD).....	15
18. TRANFER OF INFORMATION	15
19. MONITORING	16
20. SECURITY INCIDENT MANAGEMENT.....	16
21. CHANGE CONTROL.....	16
22. SOFTWARE AUTHENTICATION AND LICENSING	18
23. ANNEXURE A: IMPLEMENTATION ROADMAP	19
24. ANNEXURE B: CHANGE CONTROL PROCESS	20
25. ANNEXURE C: REFERENCES.....	22
26. ENDORSEMENT.....	23

Document Identification

File Name	ICT Security Controls Policy
Version	Version 3.0
Sensitivity Classification	Client Confidential Information
Document Owner	Laingsburg Municipality

Preparation

Action	Name	Role/Function	Date
Prepared by:	Realdo Pedro	ICT Administrator	19\03\2024
Reviewed/Approved by:	Realdo Pedro (Reviewed)	ICT Administrator	28\03\2024

Release

Version	Data Release	Change Notice	Remarks
1.0	03\05\2016	Created and Drafted Realdo Pedro (ICT Administrator)	None
1.0	12\05\2016	Drafted Security Controls Policy approved by the Policy Committee	Policies changed and approved for council
1.1	01\06\2016	Policy approved by policy committee updated and tabled for approval for council	None
1.1	19\07\2016	Policy approved by council in council meeting and ready for implementation.	Policy approved without any remarks
1.2	09\03\2020	Reviewed and prepared for approval Realdo Pedro (ICT Administrator)	None
2.0	21\09\2020	Reviewed with ICT DLG Western Cape (via MS Teams)	None
2.0	27\10\2020	Policy approved by council in council meeting and ready for implementation.	Policy approved without any remarks
3.0	19\03\2024	Reviewed and prepared for approval Realdo Pedro (ICT Administrator)	None
3.0	28\03\2024	Policy approved by council in council meeting and ready for implementation.	Policy approved without any remarks

Glossary of Abbreviations

Abbreviation	Definition
BYOD	Bring Your Own Device
COBIT	Control Objectives for Information and Related Technology
ICT	Information and Communication Technology
IP	Internet Protocol
ISO	International Organization for Standardisation
ODBC	Open Database Connectivity
PIN	Personal Identification Number
SSH	Secure Shell
UPS	Uninterrupted Power Supply
USB	Universal Serial Bus
WPA2	Wi-Fi Protected Access 2

Glossary of Terminologies

Terminology	Definition
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, deleting users.
Biometric information	Personal information obtained through biometric measurements, such as finger prints, 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.

1. INTRODUCTION

Information security has become an increasingly important subject for the Municipality. This is driven mainly by the strategic nature of data and/or information, which serves as evidence of prevalent socio-economic issues, against which service delivery solutions will be based. The increase in cybercrimes, evolving technologies, and regulatory requirements are additional factors that give rise to the importance of employing adequate controls for securing information held by the municipality.

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 highest standards of integrity, and most importantly accessible to those who have authority to use it. For the purpose of this policy we consider information security in the context of Information and Communication Technologies (ICT).

Furthermore, this policy seeks to guide processes pertaining to capturing, processing, destruction and/or loss of data, as well as how such information ought to be disclosed to the interested parties.

2. LEGISLATIVE FRAMEWORK

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

The following legislation, among others, were 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.
- 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.
- 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, 2009

3. OBJECTIVE OF THE POLICY

The objective of the policy is to provide guidance on measures the municipality could employ in order to prevent/mitigate actions that threaten (risk) the integrity of the overall municipality through malicious attack of Municipality's ICT systems, information and infrastructure. This policy also seeks to outline the acceptable use of ICT resources by Officials and any party that renders services to, or on behalf of the Municipality to ensure that appropriate technologies are applied to strengthen the safeguarding of the institution's information. Employment of proper security controls will allow for backing up, through trusted evidence, of decisions that the Municipality makes while it advances towards achieving set goals and objective which will in turn result in betterment of ordinary citizens.

4. SCOPE

This ICT Security Controls Policy has been developed to guide and assist municipalities to be aligned with internationally recognised best practice ICT Security Controls. This policy recognizes that municipalities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of information security.

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 ICT systems of the Municipality.

Municipalities must develop their own Security controls and procedures by adopting the principles and practices presented in this policy.

The policy covers the following elements of information security:

- Ownership and classification of information;
- Security incident management;
- Physical security;
- Application security;

- Network security;
- Database security;
- Change control; and
- Software authorization and licensing.

Aspects relating to user access, server security and data backup are covered in the ICT User Access Management, ICT Operating System Security Controls and the ICT Data Backup and Recovery policies.

5. 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 in accordance with 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.

6. ADMINISTRATION OF POLICY

The 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 Council.

7. PROTECTION OF CLASSIFIED INFORMATION

- 7.1. 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 require Councillors and Officials to employ a strict level of self-discipline in order to prevent communication of sensitive or classified information. Councillors and Officials may not disclose any privileged or confidential information to an unauthorised person
- 7.2. All Municipal data must be classified in accordance with the Minimum Information Security Standards, as approved by Cabinet in 1996. Therefore all official matters requiring the application of security measures must be classified either as "Restricted" or "Confidential". By default, Municipal data has been classified as Restricted.

Classification	Description
Restricted	Information that may be used to hamper Municipal activities.
Confidential	Information that may be used harm the objectives and functions of the Municipality.

Table 1: Data classification in accordance with the MISS

- 7.3. 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.
- 7.4. Officials, in conjunction with the ICT Manager, must ensure that classified information receives adequate protection to prevent compromise.
- 7.5. Officials who generate sensitive information are responsible for determining the information classification levels. This responsibility includes the labelling of classified documents.
- 7.6. The Minimum Information Security Standards Chapter 6, Section 1 requires that a declaration of secrecy must be made on an official form during the appointment process for any government post.

8. PROTECTION OF PUBLIC RECORDS

- 8.1. The National Archives and Records Service of South Africa Act, Act 43 of 1996 requires sound records management principles to be applied to electronic records and e-mails created or received in the course of official business and which are kept as evidence of the Municipality's functions, activities and transactions. The detail of these requirements can be found in:
 - a) The [Records Management Policy], [Internet and e-Mail Usage], [Web Content Management Policy] and [Document Imaging Policy] of the Municipality; and
 - b) The National Archives and Records Service of South Africa Regulations.
- 8.2. The Records Manager is responsible for the implementation of sound records management principles and record disposal schedules for the Municipality.
- 8.3. The ICT Manager must work with the Records Manager to ensure that public records in electronic form are managed, protected and retained for as long as they are required.

- 8.4. Information security plays an important role in records management as a means to protect the integrity and confidentiality of public records. The ICT Manager must ensure that systems used for records management of electronic public records and e-mails are configured and managed as follows.
- a) Systems must capture appropriate metadata (background and technical information about the data);
 - b) The systems must establish an audit trail to log all attempts to alter or edit electronic records and their metadata;
 - c) The system must protect the integrity of records until they have reached their approved retention. Integrity of records can be accomplished through procedures such as backup test restores, media testing, data migration controls and capturing the required audit trails;
 - d) Access controls must protect records against unauthorized access and tampering;
 - e) Access controls must prevent removal of data from premises without the explicit permission of the ICT Manager;
 - f) Systems must be free from viruses;
 - g) The system must ensure that electronic records, that have to be legally admissible in court and carry evidential weight, are protected to ensure that they are authentic, not altered or tampered with, auditable and produced in systems which utilise security measures to ensure their integrity;
 - h) The ICT Manager must ensure that the suitability of new system for records management are assessed during its design phase. The Records Manager must be involved during the design specification.

9. PROTECTION OF PERSONAL INFORMATION

- 9.1. 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.
- 9.2. The Promotion of Access to Information Act, Act No. 2 of 2000, gives effect to the right to access personal information held by the Municipality and must be complied with.
- 9.3. The Protection of Personal Information Act, Act No. 4 of 2013, gives effect to the right to privacy. The Act requires that the Information Officer of the Municipality ensure that personal information are lawfully obtained and processed.

- 9.4. The ICT Manager and Officials must work together to ensure the following with respect to 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 are 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”).
- 9.5. The Protection of Personal Information Act, No. 4 of 2013, Section 6, contains certain general exceptions where the Act does not apply e.g. the processing of personal information for national security, defence, public safety, law enforcement or for the judicial functions of a court.
- 9.6. The Protection of Personal Information Act, No. 4 of 2013 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) have given consent, or if an exception apply. Examples are shown hereunder (refer to the Act for further detail):

Sections	Special personal information	Collection and processing prohibited unless exceptions apply. Examples of exceptions provided:
Sections 6, 34 to 37	Children’s information	Establishment or protection of a right of the child.
Sections 6 & 28	Religious or philosophical beliefs	To protect the spiritual welfare of a community.

Sections	Special personal information	Collection and processing prohibited unless exceptions apply. Examples of exceptions provided:
Sections 6 & 29	Race or ethnic origin	Protection from unfair discrimination or promoting the advancement of persons.
Sections 6 & 30	Trade union membership	To achieve the aims of trade union that the person belongs to.
Sections 6 & 31	Political persuasion	To achieve the aims of a political institution that the person belongs to.
Sections 6 & 32	Health or sex life	Provision of healthcare services, special support for pupils in schools, childcare or support for workers.
Sections 6 & 33	Criminal behaviour or biometric information	Necessary for law enforcement.

Figure 1 : Special personal information protected by the Protection of Personal Information Act, No. 4 of 2013

9.7. The following personal information are 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.

9.8. The Promotion of Access to Information Act, Act No. 2 of 2000, 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 defence, security and international relations of the Republic;
 - Information that will jeopardise the economic interests and financial welfare of the Republic and commercial activities of the Municipality;
 - Research information of the Municipality; and
 - Information about the operations of the Municipality;
- 9.9. The Promotion of Access to Information Act, Act No. 2 of 2000, require that information relating to public safety, environmental risk, or a substantial contravention of, or failure to comply with the law, be disclosed immediately;

10. PROTECTION OF RECORDS TO PRESERVE LEGALITY

- 10.1. The Electronic Communications and Transactions Act, Act. No. 25 of 2002, prescribes information security controls to preserve the evidential weight of electronic records and e-mails.
- 10.2. The evidential weight of electronic records and e-mails is a continuum, where the weight of the evidence increases with the number of information security controls applied. The following lists examples of such specific information security controls:
- Restrict access to records
 - Encrypt records
 - Store records on write once, read many times, media
 - Apply records management principles
 - Store records in a database management system
 - Apply change control to the records management system
 - Backup data
 - Use digital certificates to confirm the identities of senders and receivers of messages

11. GENERAL CONTROL ENVIROMENT

- 11.1. To ensure 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 unauthorised 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. Refer to the ICT User Access Management Policy for the requirements relating to user access, applications.

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 prior to disposal or re-use.
- 12.5. Any hardware that carry 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 standardised as far as possible to promote fast, reliable and cost-effective ICT service delivery to the Municipality.

13. DATABASE SECURITY

- 13.1. The ICT Manager must limit full access to databases (e.g. sysadmin server role, db_owner database role, sa built-in login etc.) to ICT staff who need this access. Officials who use applications may not have these rights to the application's databases.
- 13.2. The ICT Manager must ensure that Officials who access databases directly (e.g. through ODBC) only have read access.
- 13.3. The ICT Manager must review database rights and permissions on a quarterly basis. Excessive rights and permissions must be removed.

14. NETWORK SECURITY

- 14.1. The ICT Manager must document the network structure and configuration including IP addresses, location, make and model of all hubs, switches, routers and firewalls.
- 14.2. The ICT Manager must implement a firewall between the Municipal network and other networks
- 14.3. The ICT Manager must limit administrator access to the firewall and user accounts must have strong passwords of at least 8 characters with a combination of alpha-numeric characters and symbols. Remote firewall administration is only allowed using SSHv2 from the internal network.
- 14.4. The ICT Manager must configure the firewall to block all incoming ports, unless the service is required to connect to a server on the internal network (e.g. port 80 and port 443 for web servers). When an incoming port is allowed, the service may only connect to the specific servers on the internal network. Internal IP addresses may not be visible outside of the internal network.
- 14.5. The ICT Manager must set the firewall to block intrusion attempts. The ICT Manager must raise an incident and deal with the root causes of the event.
- 14.6. The ICT Manager must place infrastructure, user devices (e.g. personal computers) and servers facing externally on separate network domains.
- 14.7. The ICT department must scan the entire network with security software on a monthly basis to detect security vulnerabilities. The scans must be performed from the Internet, as well as from the internal network.
- 14.8. Officials and the ICT Manager must remove all modems from the internal network to avoid intruders bypassing the firewall.
- 14.9. System administrators must install personal firewalls on laptops and personal computers. Officials may not disable these firewalls. Officials must choose to deny a specific address when prompted by the personal firewall, unless approved by ICT.
- 14.10. The ICT department must ensure that all inactive network points are disabled.

15. E-MAIL AND INTERNET

- 15.1. 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 Internet may not be used for any illegal or offensive activities.
- 15.2. 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.

16. WIRELESS NETWORKS

- 16.1. System administrators must configure all wireless networks to the following standard:
 - WPA2 security protocol or better;
 - Password strength of at least 8 characters with a combination of alpha-numeric characters and symbols;
 - The latest firmware must be installed; and
 - Default system usernames and passwords must be removed.
- 16.2. Officials may not set up wireless networks that are attached to the internal network.

17. MOBILE DEVICES AND OWN HARDWARE (BYOD)

- 17.1. The ICT Manager must approve all hardware and software, owned by Officials and service providers, which is to be used for official purposes.
- 17.2. The ICT team must ensure that all mobile devices must be protected with a PIN.

18. TRANSFER OF INFORMATION

- 18.1. The ICT Manager must ensure that classified information may only be transmitted over external networks using encryption.
- 18.2. Officials may not use personal storage devices (e.g. USB memory sticks or portable hard drives) to store Municipal data. When required for official purposes, these devices must be encrypted by the ICT team.

19. MONITORING

- 19.1. The Municipal Manager authorises the monitoring of Municipal systems by the ICT Manager.
- 19.2. Municipal officials must be made aware that the network is being monitored to ensure network security, to track the performance of the network and systems, and to protect the network from viruses.

20. SECURITY INCIDENT MANAGEMENT

- 20.1. All Municipal users must report actual or suspected security breaches or security weaknesses to the ICT Manager or the delegated authority.
- 20.2. The ICT Manager must record all information regarding security incidents. The ICT Manager must review all the information security incidents on a quarterly basis to ensure that the root cause of the problems are addressed.
- 20.3. Investigations into security incidents may only be carried out by the ICT Manager or a nominated person.
- 20.4. The Protection of Personal Information Act, Act No. 4 of 2013 prescribe that the Regular and the person affected by the breach must be notified in the event of a breach of personal information.

21. CHANGE CONTROL

- 21.1. 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 afterwards. 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 in the most effective way.
 - d) Recurring operational tasks are excluded from the structured change control process

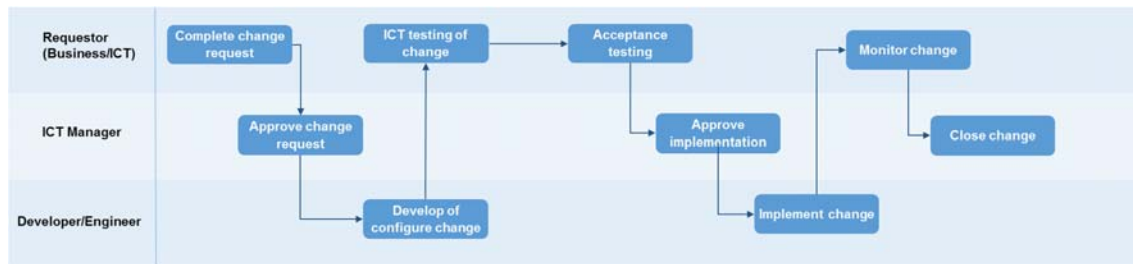
- 21.2. The following additional rules with respect to change control must be adhered to. In some cases this may not be cost-effective or technically possible, in which case it is the duty of the ICT Manager to review and approve alternative controls.
- a) The same person who performs the change may not implement the change.
 - b) Systems must have a development environment where testing is conducted to avoid testing in the production environment.
 - c) If a vendor performs the change, the Municipality must also test the change.
 - d) The data inside a database may not be edited, except through an approved application front-end. This excludes internal system processes or interfaces, or work required to convert data during a system implementation.
 - e) Commercial software must be selected after considering information security requirements.
 - f) The affected user's willingness to change must always be considered when documenting all that can go wrong with the change.
 - g) Any system published to the Internet or on a mobile platform must be reviewed by security specialists before being deployed.
- 21.3. The ICT Manager must record all change requests across the Municipality in a central tool, file server or spreadsheet. This implies that changes performed by ICT and those changes requested by the business from vendors, without ICT involvement, must be recorded together.
- 21.4. The ICT Manager must create a weekly report which lists all of the unapproved change requests, active changes requests, cancelled change requests and completed change requests. The report must be reviewed, and actions taken, to ensure that:
- Change requests receive sufficient attention;
 - The change control process is being followed for all known changes; and
 - Trends across change requests, that indicate systemic problems in the ICT environment, are identified and require more permanent fixes

22. SOFTWARE AUTHENTICATION AND LICENSING

- 22.1. The ICT Manager must retain a record of all licenses owned by the Municipality.
- 22.2. The ICT Manager must scan all ICT resources on an annual basis to verify that only authorised software is installed.
- 22.3. The ICT Steering Committee must approve all software being used in the Municipality. An approved software list must be maintained by the ICT Manager and approved by the ICT Steering Committee.
- 22.4. The ICT Steering Committee may only authorise software from known, reputable sources to reduce the likelihood of introducing errors or security risks into the environment.
- 22.5. Officials may not install or change the software on their computers.

24. ANNEXURE B: CHANGE CONTROL PROCESS

24.1. The diagram below depicts the structured change control process:



The structured change control process must include the following steps:

Step	Description
1. Complete change request	<p>Complete a change request (electronic or paper-based). The change request form must include the following information:</p> <ul style="list-style-type: none"> A unique number, which runs in a sequence. Who requested the change? Who approves the change? A description of the change in business terms. A description of the change translated from business terms into specific ICT components that will be changed. The cost and resources required to perform the change. All that can go wrong with the change. What must be done to avoid all that can go wrong? Roll back plans
2. Approve change request	Seek approval of the change request from the requester and record this on the change request.
3. Develop or configure change	Develop or configure the change to the point where it is ready for testing.
4. ICT testing of change	Test the change from a development or configuration perspective, paying particular attention to prevent all that can go wrong with the change.
5. Acceptance testing	Requester to test the change to determine if the requirement has been met. Pay attention to prevent all that can go wrong with the change.

Step	Description
6. Approve implementation	Seek approval from the requester to implement the change request, and record this on the change request.
7. Implement the change	Implement the change.
8. Monitor the change	Monitor the change for a period of time to ensure that it was successful.
9. Close the change	Seek approval from the requester to close the change request, and record this on the change request.

Table 2 : Change control process, step by step

25. ANNEXURE C: REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.

Constitution of the Republic of South Africa. (1996). Republic of South Africa.

Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.

Copyright Act No. 98. (1978). Republic of South Africa.

King Code of Governance for South Africa. (2009). Institute of Directors in Southern Africa.

Local Government: Municipal Finance Management Act, No. 53. (2003). Republic Of South Africa.

Local Government: Municipal Structures Act 117. (1998). Republic of South Africa.

Local Government: Municipal Systems Act 32. (2000). Republic of South Africa.

Minumum Information Security Standards. (1996, December 4). Cabinet.

Promotion of Access to Information Act 2. (2000). Republic of South Africa.

Protection of Personal Information Act, No. 4. (2009). Republic of South Africa.


Regulation of Interception of Communications and Provision of Communication-Related Information Act 70. (2002). Republic of South Africa.

26. ENDORSEMENT

The Municipal Manager / Accounting Officer by virtue of his signature hereby Endorse this policy.

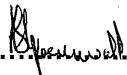
The Mayor / Speaker by virtue of his signature, on behalf of the Council of Laingsburg Municipality and after presentation of this policy before Council hereby Approve this policy.

Compiled by:


.....
REALDO PEDRO
ICT Administrator

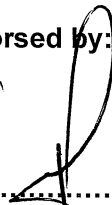
03 April 2024
DATE

Recommended by:


.....
ALIDA GROENEWALD
Chief Financial Officer


03 April 2024
DATE

Endorsed by:


.....
JAFTA BOOYSEN
Municipal Manager

03 April 2024
DATE

Approved by on behalf of Council of Laingsburg Municipality.


.....
Mayor/Speaker

03 April 2024
DATE