# ICT SECURITY CONTROLS POLICY

TABLE OF CONTENTS

## 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 is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that the Municipality's ICT systems, data and infrastructure are protected from risks such as unauthorised access (see ICT User Access Management Policy for further detail), manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

## 2. 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, 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 internationally 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 reduce the risk of harm that can be caused to the Municipality's ICT systems, information and infrastructure. This policy also seeks to outline the acceptable use of ICT resources by Officials and 3rd party service providers, to ensure that the investment in modern technology is applied to the best advantage of the Municipality.

This policy defines the collective controls to prevent Information Security related risk from hampering the achievement of the Municipality's strategic goals and objectives.

## 4. AIMS OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms to a standard set of security controls for information security in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of Information Security are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

## 5. 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 authorisation 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.

## 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 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.

## 7. 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.

## 8. PROTECTION OF CLASSIFIED INFORMATION

8.1 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.

8.2 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. |

| Classification | Description |
|---|---|
| Confidential | Information that may be used harm the objectives and functions of the Municipality. |

**Table 1: Data classification in accordance with the MISS**

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 labelling of classified documents.

8.6 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.

## 9. PROTECTION OF PUBLIC RECORDS

9.1 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.

9.2 The Records Manager is responsible for the implementation of sound records management principles and record disposal schedules for the Municipality.

9.3 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.

9.4 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) Access to server rooms and storage areas for electronic records media must be restricted to ICT staff with specific duties regarding the maintenance of the hardware, software and media.

(i) Systems technical manuals and systems procedures manuals must be designed for each system.

(j) A systems technical manual include information regarding the hardware, software and network elements that comprise the electronic record keeping system and how they interact. Details of all changes to a system must also be documented.

(k) A system procedures manual include all procedures relating to the operation and use of the system, including input to, operation of and output from the system. A systems procedures manual should be updated when new releases force new procedures.

(l) 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.

## 10. PROTECTION OF PERSONAL INFORMATION

10.1 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.

10.2 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.

10.3 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.

10.4 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").

10.5 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.

10.6 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 6 & 29 | Race or ethnic origin | Protection from unfair discrimination or promoting the advancement of persons. |

| Sections | Special personal information | Collection and processing prohibited unless exceptions apply. Examples of exceptions provided: |
|---|---|---|
| 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**

10.7 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.

10.8 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.

10.9 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.

## 11. PROTECTION OF RECORDS TO PRESERVE LEGALITY

11.1 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.

11.2 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

## 12. GENERAL CONTROL ENVIRONMENT

12.1 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.

12.2 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.

12.3 Refer to the ICT User Access Management Policy and the ICT Operating System Security Controls Policy for the requirements relating to user access, applications and operating system security.

## 13. PHYSICAL SECURITY

13.1 The ICT Manager must take reasonable steps to protect all ICT hardware from natural and man-made disasters to avoid loss and ensure reliable ICT service delivery. ICT hardware under control of the ICT function must be hosted in server rooms or lockable cabinets. Server rooms must be of solid construction and locked at all times.

13.2 The ICT department must retain an access control list for the server room. Access must be reviewed quarterly by the ICT Manager.

13.3 All server rooms must be equipped with air-conditioning, UPS and fire detection and suppression.

13.4 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.

13.5 Server rooms must be kept clean to avoid damage to hardware and reduce the risk of fire.

13.6 Cabling must be neat and protected from damage and interference.

13.7 No ICT equipment may be removed from the server room or offices without prior authorisation from the ICT Manager.

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

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

13.10 All data and software on hardware must be erased prior to disposal or re-use.

13.11 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.

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

13.13 The off-site location, used to store backup data media, must be protected with the following physical security measures:

- Building of solid construction;
- Physical access control;
- Fire detection and suppression; and
- Environmental conditions adhere to vendor recommendations for storage of media.

## 14. DATABASE SECURITY

14.1 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.

14.2 The ICT Manager must ensure that Officials who access databases directly (e.g. through ODBC) only have read access.

14.3 The ICT Steering Committee must approve all instances where Officials have edit or execute access to databases.

14.4 The ICT Manager must review database rights and permissions on a quarterly basis. Excessive rights and permissions must be removed.

## 15. NETWORK SECURITY

15.1 The ICT Manager must document the network structure and configuration including IP addresses, location, make and model of all hubs, switches, routers and firewalls.

15.2 The ICT Manager must implement a firewall between the Municipal network and other networks.

15.3 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.

15.4 The ICT Manager must check and install firewall upgrades and patches on a weekly basis. An obsolete firewall (one that is not supported by the vendor any longer and / or has known security vulnerabilities) must be replaced.

15.5 The ICT Manager must document the firewall rulesets and configuration settings. The rulesets and configuration settings must be reviewed quarterly to ensure that it remains current (i.e. remove unused services) and that services that expose the Municipality to security risk are reviewed continuously.

15.6 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.

15.7 The ICT Steering Committee must approve all open incoming ports. The ICT Steering Committee must only approve requests that are absolutely necessary and with consideration of the associated security risks.

15.8 The system administrators must set the firewall to block intrusion attempts and to alert the ICT Manager when additional action needs to be taken. The ICT Manager must raise an incident and deal with the root causes of the event.

15.9 The ICT Manager must place infrastructure, user devices (e.g. personal computers) and servers facing externally on separate network domains.

15.10 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.

15.11 Officials and the ICT Manager must remove all modems from the internal network to avoid intruders bypassing the firewall.

15.12 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.

15.13 The ICT department must ensure that all inactive network points are disabled.

## 16. E-MAIL AND INTERNET

16.1 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.

16.2 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.

## 17. WIRELESS NETWORKS

17.1 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.

17.2 Officials may not establish wireless networks attached to the internal network without the consent of the ICT Manager. All wireless networks must adhere to the secure configuration standard.

## 18. MOBILE DEVICES AND OWN HARDWARE (BYOD)

18.1 The ICT Manager must approve all hardware and software, owned by Officials and service providers, which is to be used for official purposes.

18.2 The ICT team must ensure that all mobile devices must be protected with a PIN.

## 19. TRANSFER OF INFORMATION

19.1 The ICT Manager must ensure that classified information may only be transmitted over external networks using encryption.

19.2 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, and the data is of a confidential nature, these devices must be encrypted by the ICT Manager.

## 20. MONITORING

20.1 The Municipal Manager authorises the monitoring of Municipal systems by the ICT Manager.

20.2 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.

20.3 If users give their written consent, any e-mail, Internet and other network service may be monitored. A signed acceptable user agreement is required in order to achieve this consent.

## 21. SECURITY INCIDENT MANAGEMENT

21.1 All Municipal users must report actual or suspected security breaches or security weaknesses to the ICT Manager or the delegated authority.

21.2 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.

21.3 Investigations into security incidents may only be carried out by the ICT Manager or a nominated person.

21.4 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.

## 22. CHANGE CONTROL

22.1 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 help-desk processes designed to deliver ICT services in the most effective way.

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

22.2 The ICT Manager must establish the formal change control process. Refer Appendix B, Change Control Process.

22.3 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 Steering Committee 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 reviewed by security specialists before being deployed.

22.4 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.

22.5 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.

## 23. SOFTWARE AUTHORISATION AND LICENSING

23.1 The ICT Manager must retain a record of all licenses owned by the Municipality.

23.2 The ICT Manager must scan all ICT resources on an annual basis to verify that only authorised software is installed.

23.3 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.

23.4 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.

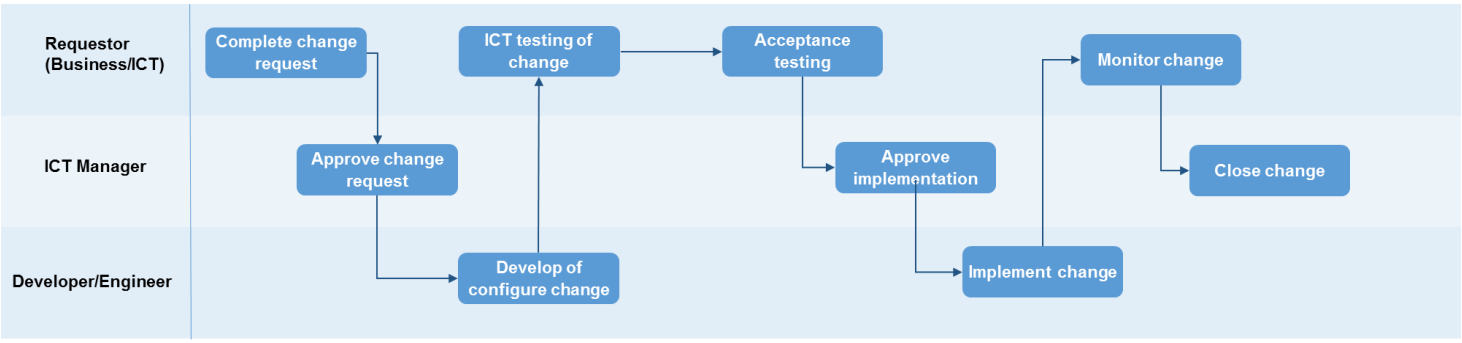
23.5 Officials may not install or change the software on their computers.

## 24. ANNEXURE A: IMPLEMENTATION ROADMAP

| No | Action | Month 1 | Month 2 | Month 3 | Month 4 | Month 5 | Month 6 | Month 7 | Month 8 | Month 9 | Month 10 | Month 11 | Month 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Allocate the information security role | | | | | | | | | | | | |
| 2 | Create an inventory of information that require protection | | | | | | | | | | | | |
| 3 | Perform a gap analysis against the controls in the policy | | | | | | | | | | | | |
| 4 | Create Acceptable Use Policy for IT | | | | | | | | | | | | |
| 5 | Obtain approval from ICT Steering Committee for improvements | | | | | | | | | | | | |
| 6 | Provide security awareness | | | | | | | | | | | | |
| 7 | Implement change control | | | | | | | | | | | | |
| 8 | Implement server room security | | | | | | | | | | | | |
| 9 | Implement user hardware / software use controls | | | | | | | | | | | | |
| 10 | Implement database security | | | | | | | | | | | | |
| 11 | Implement network security | | | | | | | | | | | | |
| 12 | Implement e-mail and Internet security | | | | | | | | | | | | |
| 13 | Implement wireless security | | | | | | | | | | | | |
| 14 | Implement mobile device security | | | | | | | | | | | | |
| 15 | Implement information transfer controls | | | | | | | | | | | | |
| 16 | Implement software licensing | | | | | | | | | | | | |
| 17 | Implement security incident management | | | | | | | | | | | | |
| 20 | Commence operational security management | | | | | | | | | | | | |

## 25. ANNEXURE B: CHANGE CONTROL PROCESS

25.1 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 | Complete a change request (electronic or paper-based). The change request form must include the following information:<br>• A unique number, which runs in a sequence.<br>• Who requested the change.<br>• Who approves the change.<br>• A description of the change in business terms.<br>• A description of the change translated from business terms into specific ICT components that will be changed.<br>• The cost and resources required to perform the change.<br>• All that can go wrong with the change.<br>• What must be done to avoid all that can go wrong.<br>• 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. |

| Step | Description |
|---|---|
| 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. |
| 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**

## 26. 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.