



ICT SECURITY CONTROLS POLICY

1 July 2024

TABLE OF CONTENTS

1.	ABBREVIATIONS	2
2.	PURPOSE OF THIS POLICY	3
3.	LEGISLATIVE FRAMEWORK	3
4.	SCOPE	4
5.	SECURITY USER AWARENESS	5
6.	GENERAL CONTROL ENVIRONMENT	5
7.	DOCUMENTS THAT SHOULD BE READ WITH THIS POLICY	6
8.	ROLES AND RESPONSIBILITIES	6
9.	PHYSICAL SECURITY	8
10.	DATABASE SECURITY	9
11.	NETWORK SECURITY	10
12.	E-MAIL AND INTERNET	11
13.	TELEPHONE AND FAX	13
14.	DATA MANAGEMENT	13
15.	WIRELESS NETWORKS	15
16.	MOBILE DEVICES AND OWN HARDWARE (BYOD)	15
17.	INFORMATION SYSTEMS	15
18.	SOFTWARE	16
19.	SOFTWARE PATCH MANAGEMENT	17
20.	PASSWORD MANAGEMENT	18
21.	INVALID LOGIN ATTEMPTS	19
22.	TRANSFER OF INFORMATION	19
23.	MONITORING	20
24.	SECURITY INCIDENTS MANAGEMENT	20
25.	CHANGE CONTROL	21
26.	BREACH OF POLICY	22
27.	REVIEW OF POLICY	24

1. ABBREVIATIONS

“**SWDM**” refers to Swellendam Municipality.

“**ICT Services Division**” refers to Swellendam ICT Department and its staff members.

“**Site Manager**” refers to anyone appointed as the head of technical operations.

“**Manager ICT Services**” refers to the Head of the ICT Services Division

“**COBIT**” refers to Control Objectives for Information and Related Technology

“**ICT**” refers to Information and Communication Technology

“**ITIL**” refers to ICT Infrastructure Library

“**SIP**” refers to a Service Improvement Plan

“**CRF**” refers to Change Request Forms.

“**Email**” refers to electronic mail.

“**CFO**” refers to Director Financial Services.

“**HOD**” refers to the Manager or Head of Division.

“**BYOD**” refers to Bring Your Own Device

“**IP**” refers to Internet Protocol

“**ISO**” refers to International Organization for Standardisation

“**PIN**” refers to Personal Identification Number

“**SSH**” refers to Secure Shell

“**UPS**” refers to Uninterrupted Power Supply

“**USB**” refers to Universal Serial Bus

“**WPA2**” refers to Wi-Fi Protected Access 2

2. PURPOSE OF THIS POLICY

- 2.1 The purpose of this policy is to control access and changes to the Council ICT resources and to safeguard and control SWDM ICT Infrastructure.
- 2.2 This policy serves to guide all who are responsible for effecting changes to ICT Infrastructure for purposes of investigation, analyzing, assessing, testing and implementing changes. This policy seeks to minimize disruption to ICT services at SWDM.
- 2.3 Information security ensures that the SWDM ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as the unauthorised disclosure or incorrect processing of data.
- 2.4 This policy ensures that the SWDM 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 risks associated with the management of Information Security are mitigated.
- 2.5 This policy supports the Municipality's Corporate Governance of ICT Policy.

3. LEGISLATIVE FRAMEWORK

- 3.1 The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognised ICT standards. The following legislation, among others, was considered in the drafting of this policy:
 - 3.1.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
 - 3.1.2 Copyright Act, Act No. 98 of 1978;
 - 3.1.3 Electronic Communications and Transactions Act, Act No. 25 of 2002;
 - 3.1.4 Minimum Information Security Standards, as approved by Cabinet in 1996;
 - 3.1.5 Municipal Finance Management Act, Act No. 56 of 2003;
 - 3.1.6 Municipal Structures Act, Act No. 117 of 1998;

- 3.1.7 Municipal Systems Act, Act No. 32, of 2000;
- 3.1.8 Provincial Archives and Record Service of South Africa Act, Act No. 3 of 2005;
- 3.1.9 Provincial Archives Regulations and Guidelines;
- 3.1.10 Promotion of Access to Information Act, Act No. 2 of 2000;
- 3.1.11 Protection of Personal Information Act, Act No. 4 of 2013;
- 3.1.12 Regulation of Interception of Communications Act, Act No. 70 of 2002;
- 3.1.13 Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005;
- 3.1.14 Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
- 3.1.15 Control Objectives for Information Technology (COBIT) 5, 2012;
- 3.1.16 ISO 27002:2013 Information technology — Security techniques Code of practice for information security controls;
- 3.1.17 King IV - Code of Governance Principles.

4. SCOPE

- 4.1 The policy applies to everyone in the SWDM, including its 3rd party service providers and consultants.
- 4.2 This policy is regarded as being critical to the security of the ICT systems of the Municipality.
- 4.3 The policy covers the following elements of information security:
 - 4.3.1 Security Incident Management;
 - 4.3.2 Physical security;
 - 4.3.3 Application security;
 - 4.3.4 Network security;
 - 4.3.5 Database security;
 - 4.3.6 Change control; and
 - 4.3.7 Software authorisation and licensing.
- 4.4 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. SECURITY USER AWARENESS

- 5.1 Every councillor, employee, contractor and authorized 3rd party entity should become familiar with this Policy's provisions and the importance of adhering to it when effecting changes to SWDM ICT Infrastructure.
- 5.2 This policy will be sent using email to all users of ICT services and it is expected of all users to familiarize themselves with the contents and provisions of this policy.
- 5.3 The ICT Services Division must ensure that by requesting for changes to be effected and signing the change control form, this policy was read and understood.
- 5.4 Permanent Employees are to be provided with Information Security awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards;
- 5.5 An appropriate summary of the Information Security Policies must be formally delivered to, and accepted by, all temporary Employees before they started any work for the SWDM;
- 5.6 The Municipality is committed to providing regular and relevant Information Security awareness communications to all Employees by various means, such as electronic updates, briefings, newsletters, etc.;
- 5.7 All Employees are to receive Information Security awareness training. The Information Policy must form part of all employees' induction conducted by the SWDM.

6. GENERAL CONTROL ENVIRONMENT

- 6.1 The SWDM has a legal right and duty to:
 - 6.1.1 Protect its Information Assets from internal and external information security threats;
 - 6.1.2 Secure its network, data and communications;
 - 6.1.3 Protect the privacy, dignity and free speech of the public and private data collected from the public;

- 6.1.4 Ensure that the information system is available, operational and safe;
- 6.1.5 Provide awareness to its employees regarding information security risks and liabilities;
- 6.1.6 Foster awareness of information security threats;
- 6.1.7 Comply with new information technology and data protection legislation; and
- 6.1.8 To protect the SWDM Business Information and any consumer Information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability;
- 6.1.9 To establish responsibility and accountability for information security in the SWDM;
- 6.1.10 To encourage management and Employees to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of information security incidents;
- 6.1.11 To ensure that the SWDM can continue its commercial activities in the event of significant information security Incidents.
- 6.1.12 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 unauthorised access to Municipal data.

7. DOCUMENTS THAT SHOULD BE READ WITH THIS POLICY

- 7.1 ICT Standard Operating Procedure.
- 7.2 ICT Equipment and Allocation Policy
- 7.3 ICT User and Network Access Policy
- 7.4 SWDM Asset Management Polic
- 7.5 ICT Remote Access Policy
- 7.6 ICT Data Backup and Recovery Policy.
- 7.7 ICT Software Patch Policy

8. ROLES AND RESPONSIBILITIES

- 8.1 All SWDM ICT Services Team members are responsible to make sure that they are providing access and effecting changes in compliance with the Municipality's ICT Information Security Policy. It is the responsibility of

every user of ICT Infrastructure to ensure adherence to this Information Security Policy.

- 8.2 SWDM ICT Services is responsible for informing users of prospective changes that affect them through email and their Directors and/or Managers whichever is applicable or both.
- 8.3 All Employees must treat passwords as private and highly confidential. Employees may not disclose their own passwords to anyone. Non-compliance with this policy could result in disciplinary action;
- 8.4 Employees may not attempt to discover another person's password;
- 8.5 All Employees are responsible for all system activity conducted under their User ID;
- 8.6 No Employee may tamper with any security settings on any computer that may endanger the Municipality, including but not limited to removal of screen-savers, removal of anti-virus software, etc;
- 8.7 Employees may not attempt to illegally gain access to another user's files and/or another site's computer facilities;
- 8.8 All software and/or licensing copyright requirements must be strictly adhered to by all Employees;
- 8.9 No new Software packages or downloads must be installed by any employee. Only the ICT Services Division is allowed to install software or any other applicable downloads.
- 8.10 Confidential Information should be shared only with other authorised persons;
- 8.11 The ICT Manager and or delegate must sign for the receipt of all computer equipment and or goods. They are to ensure that, by signing for them, they are considered to be verifying the correct quantity, quality and condition of the goods according to the order issued;
- 8.12 Employees must sign for the receipt of computer equipment and or goods provided at their workstations. They are to ensure that, by signing

for them, they are considered to be verifying the quantity, quality and condition of the goods issued;

- 8.13 Only authorised persons may sign for work done by third parties;
- 8.14 Only the ICT Manager per the delegated authority may order ICT infrastructure and computer equipment on behalf of the Municipality;
- 8.15 Telephone enquiries for Sensitive or Confidential Information are to be referred to management. Only authorised persons may disclose Information classified for Public Information in terms of the POPIA Act;
- 8.16 All data and information not in the public domain, relating to the SWDM and its Employees, must remain confidential at all times;
- 8.17 The playing of games on office PCs or laptops is prohibited; and
- 8.18 Using the Municipality's computers for personal/private business is strongly discouraged.

9. PHYSICAL SECURITY

- 9.1 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.
- 9.2 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.
- 9.3 The security alarm company must provide a user access list once a month for the access to be monitored and verified. The user access list must be available to the Internal Auditor upon request.
- 9.4 All server rooms must be equipped with air-conditioning, UPS and fire detection and suppression. (fire detection to be installed later)
- 9.5 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.

- 9.6 A call logging system must be in place to control any changes or maintenance in the ICT department.
- 9.7 Server rooms must be kept clean to avoid damage to hardware and reduce the risk of fire.
- 9.8 Cabling must be neat and protected from damage and interference.
- 9.9 No ICT equipment may be removed from the server room or offices without prior authorisation from the ICT Manager.
- 9.10 All hardware owned by the Municipality must be returned by employees and service providers when no longer needed or on termination of their contract.
- 9.11 All data and software on hardware must be erased before disposal or re-use.
- 9.12 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.
- 9.13 ICT hardware and software must be standardised as far as possible to promote fast, reliable and cost-effective ICT service delivery to the Municipality.
- 9.14 The off-site location, used to store backup data media, must be protected with the following physical security measures: (To be implemented once established)
 - 9.14.1 Building of solid construction;
 - 9.14.2 Physical access control;
 - 9.14.3 Fire detection and suppression; and
 - 9.14.4 Environmental conditions adhere to vendor recommendations for the storage of media.

10. DATABASE SECURITY

- 10.1 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.

- 10.2 The ICT Manager must ensure that Officials who access databases directly (e.g. through ODBC) only have read access.
- 10.3 The ICT Manager with CFO must approve all instances where Officials have edited or executed access to databases.
- 10.4 The ICT Manager must review database rights and permissions quarterly. Excessive rights and permissions must be removed.

11. NETWORK SECURITY

- 11.1 The ICT Manager must document the network structure and configuration including IP addresses, location, make and model of all hubs, switches, routers and firewalls.
- 11.2 The ICT Manager must implement a firewall between the Municipal network and other networks.
- 11.3 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.
- 11.4 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.
- 11.5 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.
- 11.6 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.

- 11.7 The ICT Manager must approve all open incoming ports. Only absolutely necessary requests and with consideration of the associated security risks must be approved.
- 11.8 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.
- 11.9 The ICT Manager must place infrastructure, user devices (e.g. personal computers) and servers facing externally on separate network domains.
- 11.10 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.
- 11.11 Officials and the ICT Manager must remove all modems from the internal network to avoid intruders bypassing the firewall.
- 11.12 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.
- 11.13 The ICT department must ensure that all inactive network points are disabled.

12. E-MAIL AND INTERNET

- 12.1 The ICT Manager must make all users aware of the safe and responsible use of e-mail and Internet services. E-mail and the 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.

-
- 12.2 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.
 - 12.3 The transmission of Sensitive and Confidential Information is to be Authenticated by the use of Digital Signatures whenever possible;
 - 12.4 Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible Viruses or other Malicious Code;
 - 12.5 Data retention periods for e-mail must be established to meet legal and business requirements and must be adhered to by all Employees as detailed in the Municipality Records Management Policy;
 - 12.6 ICT Service Division responsible for setting up internet/intranet access must ensure that any access restrictions pertaining to the data in source systems are also applied to access from the SWDM Intranet;
 - 12.7 ICT Service Division is responsible for setting up Internet access are to ensure that the Municipality's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured Firewall.
 - 12.8 Unsolicited e-mail is to be treated with caution and not responded to;
 - 12.9 The ICT Services Division is responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security Incidents;
 - 12.10 Web browsers are to be used in a secure manner by making use of the built-in security features of the software concerned. the Municipality's ICT Services Division must ensure that Employees are made aware of the appropriate settings for the software concerned;
 - 12.11 Information obtained from Internet sources should be verified before being used for municipal purposes;
 - 12.12 The website is an important marketing and information resource for the SWDM and its safety from unauthorised intrusion is a top priority. Only

qualified authorised persons may be developed and amend the website with all changes being documented and reviewed;

- 12.13 The Municipality's ICT Services will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by Employees. Reports of attempted access will be scrutinised by management regularly; and
- 12.14 Computer files received from unknown senders are to be deleted without being opened.

13. TELEPHONE AND FAX

- 13.1 Conference calls are only permitted if Employees are aware of the Information Security issues involved;
- 13.2 Video conference calls are only permitted if Employees are aware of the Information Security issues involved;
- 13.3 All parties are to be notified in advance whenever telephone conversations are to be recorded;
- 13.4 Any fax received in error is to be returned to the sender. Its contents must not be disclosed to other parties without the sender's permission;
- 13.5 The identity of persons requesting Sensitive or Confidential Information over the telephone must be verified, and they must be authorised to receive it in terms of the POPIA;
- 13.6 Fax covering pages must be used on all manual faxes.

14. DATA MANAGEMENT

- 14.1 Sensitive, Private, or Confidential Information may only be transferred across networks, or copied to other media when the confidentiality and integrity of the data can be reasonably assured;
- 14.2 Day-to-day data storage must ensure that current data is readily available to authorised users and that archives are both created and accessible in case of need;

-
- 14.3 The integrity and stability of the SWDM databases must be maintained at all times;
 - 14.4 The use of removable media disks e.g. flash drives and CD-ROMs must be scanned before use for viruses and other malware.
 - 14.5 Existing directory and folder structures may only be amended by the ICT Manager with the appropriate authorisation. Access restrictions to such directories should be applied as necessary to restrict unauthorised access.
 - 14.6 The archiving of documents must take place with due consideration for legal, regulatory and municipal issues with liaison between technical and business Employees as detailed in the Municipality Records Management Policy.
 - 14.7 The Information created and stored by the Municipality's information systems must be retained for a minimum period that meets both legal and municipal requirements as detailed in the Municipality Records Management Policy;
 - 14.8 Only authorised employees may access Private, Sensitive or Confidential Information on projects owned or managed by the Municipality or its Employees;
 - 14.9 Consumer Information may only be updated by authorised Employees;
 - 14.10 Consumer data is to be safeguarded using a combination of technical Access Controls and robust procedures, with all changes supported by journals and internal audit trails; These are usually dealt with by other Departments and Directorates and due diligence should be taken in controlling access.
 - 14.11 All users of information systems whose job function requires them to create or amend data files must save their work on the system regularly in accordance with best practices, to prevent corruption or loss through system or power malfunction.

15. WIRELESS NETWORKS

- 15.1 System administrators must configure all wireless networks to the following standard:
- 15.1.1 WPA2 security protocol or better;
 - 15.1.2 Password strength of at least 8 characters with a combination of alphanumeric characters and symbols;
 - 15.1.3 The latest firmware must be installed; and
 - 15.1.4 Default system usernames and passwords must be removed.
- 16.2 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.

16. MOBILE DEVICES AND OWN HARDWARE (BYOD)

- 16.1 The ICT Manager in consultation with the CFO must approve all hardware and software, owned by Officials and service providers, which is to be used for official purposes.
- 16.2 The ICT Service Division must ensure that all mobile devices must be protected with a PIN.

17. INFORMATION SYSTEMS

- 17.1 Access to all systems must be authorised by the owner of the system and such access, including the appropriate Access Rights (or privileges), must be recorded in an Access Control List.
- 17.2 Access to the resources on the network must be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised;
- 17.3 Access to Operating System commands is to be restricted to those persons who are authorised to perform systems administration/management functions. Even then, such access must be operated under Dual Control requiring the specific approval of the Information Security Officer;

- 17.4 The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. Passwords shall not be shared with any other person for any reason;
- 17.5 Access controls are to be set at an appropriate level which minimises information security risks yet also allows the SWDM activities to be carried out without undue hindrance;
- 17.6 Access to information systems is to be logged and monitored to identify potential misuse of systems or Information;
- 17.7 Access to Information and documents is to be carefully controlled, ensuring that only authorised employees may have access to Sensitive Information; and
- 17.8 Access controls for Sensitive Information or high-risk systems are to be set in accordance with the value and classification of the Information Assets being protected.

18. SOFTWARE

- 18.1 The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased information security risks associated with such projects are mitigated using a combination of procedural and technical control techniques;
- 18.2 Only ICT Service Division are to install software on the SWDM systems; and
- 18.3 The disposal of software should only take place when it is formally agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time.
- 18.4 When unauthorised software is discovered on a user's computer is deleted without notice. That deletion will be recorded on the Track-IT and Change Management System.
- 18.5 Management must ensure that proper Segregation of Duties applies to all areas dealing with systems development, systems operations, or systems administration.

- 18.6 The use of live data for testing new systems or system changes may only be permitted where adequate controls for the security of the data are in place;
- 18.7 All new and enhanced systems must be fully supported at all times by comprehensive and up-to-date documentation.
- 18.8 New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available.
- 18.9 The ICT Manager must retain a record of all licenses owned by the SWDM.
- 18.10 The ICT Manager must scan all ICT resources on an annual basis to verify that only authorised software is installed.
- 18.11 An approved software list must be maintained by the ICT Manager.
- 18.12 Employees may not install or change the software on their computers.

19. SOFTWARE PATCH MANAGEMENT

- 19.1 Patch Management will minimize the security threats such as interruption, interception, modification and fabrication of the computing systems and financial systems.
- 19.2 The ICT Manager must develop a patch management policy that describes the Information Technology Services requirements for maintaining up-to-date operating system security patches on all SWDM-owned and managed workstations and servers.
- 19.3 Following is a list of responsibilities for software patch management:
 - 19.3.1 The ICT Manager will manage the patching needs for all the financial servers on the network.
 - 19.3.2 The ICT Service Provider will manage the patching needs for the Microsoft Windows servers on the network.
 - 19.3.3 The ICT Server Administrators will manage the patching needs of all workstations on the network.

19.3.4 The ICT Manager will manage the updating and patching needs of all workstations and servers installed with the antivirus system on the network.

19.3.5 The ICT Manager will be responsible for approving the major and emergency patch management deployment requests, requested through Change Management Process.

20. PASSWORD MANAGEMENT

20.1 Authorised Users are responsible for ensuring that their individual passwords are created and managed in accordance with the ICT User and Network Access Policy.

20.2 The minimum password length is 8 characters.

20.3 The ICT password history system must keep up to ten (10) previous passwords.

20.4 All authorised users will be required to change their passwords every 42 days.

20.5 Any password that is suspected to have been compromised must be changed immediately and the user must inform ICT services immediately.

20.6 If a user forgets their password, a request to change the password form must be completed and submitted to ICT Services Division.

20.7 The ICT Services Division will provide a temporary password to reset the user password. The user will be requested to insert a new password.

20.8 All system-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.

20.9 All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

20.9.1 When a user retires, resigns, is reassigned, released, dismissed, etc.

- 20.9.2 Contractor/temporary workers account, when no longer needed to perform their duties or at the end of their term.
- 20.10 Do not share passwords with anyone, Here is a list of "do not's"
 - 1.1.1. Don't reveal a password over the phone to anyone;
 - 20.10.1 Don't reveal a password in a mail message;
 - 20.10.2 Don't reveal a password to the boss;
 - 20.10.3 Don't talk about a password in front of others;
 - 20.10.4 Don't hint at the format of a password (e.g., "my family name");
 - 20.10.5 Don't reveal a password on questionnaires or security forms;
 - 20.10.6 Don't share a password with family members;
 - 20.10.7 Don't reveal a password to a co-worker while on vacation;
 - 20.10.8 Don't write passwords down and store them anywhere in your office;
 - 20.10.9 Don't store passwords in a file on ANY computer system unencrypted;

21. INVALID LOGIN ATTEMPTS

- 21.1 Invalid login attempts occur when the username or password is typed in incorrectly.
- 21.2 Usernames and passwords will be locked out from the network after **three** invalid login attempts and may only be reset after the completion of a password ticket.
- 21.3 **A screen timeout of 600 seconds, if no valid lock-in was registered.**
- 21.4 Third-Party Systems which are administered by the systems providers will determine their account lockout threshold.

22. TRANSFER OF INFORMATION

- 22.1 The ICT Manager must ensure that classified information may only be transmitted over external networks using encryption.
- 22.2 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 confidential, these devices must be encrypted by the ICT Manager.

23. MONITORING

- 23.1 The CFO authorises the monitoring of Municipal systems by the ICT Manager.
- 23.2 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.
- 23.3 Any e-mail, Internet and other network services may be monitored by the ICT Manager.

24. SECURITY INCIDENTS MANAGEMENT

- 24.1 All Municipal users must report actual or suspected security breaches or security weaknesses to the ICT Manager or the delegated authority.
- 24.2 The ICT Manager must record all information regarding security incidents.
- 24.3 The ICT Manager must review all the information security incidents on a quarterly basis to ensure that the root cause of the problems is addressed.
- 24.4 Investigations into security incidents may only be carried out by the ICT Manager or a nominated person.
- 24.5 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.
- 24.6 Employees are expected to remain vigilant for possible fraudulent activities.

24.7 The ICT Manager must report all open incidents and actions against open incidents to the CFO and weaknesses are reviewed and monitored weekly.

24.8 The ICT helpdesk shall provide feedback to individuals who reported the security incident and notify them of results.

25. CHANGE CONTROL

25.1 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 changing environment.

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

25.3 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.

25.4 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.

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

25.6 The following additional rules for change control must be adhered to. In some cases this may not be cost-effective or technically possible, in which case the ICT Steering Committee has to review and approve alternative controls:

25.6.1 The same person who performs the change may not implement the change.

25.6.2 Systems must have a development environment where testing is conducted to avoid testing in the production environment.

- 25.6.3 If a vendor performs the change, the Municipality must also test the change.
 - 25.6.4 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 system implementation.
 - 25.6.5 Commercial software must be selected after considering information security requirements.
 - 25.6.6 The affected user's willingness to change must always be considered when documenting all that can go wrong with the change.
 - 25.6.7 Any system published on the Internet or a mobile platform must be reviewed by security specialists before being deployed.
- 25.7 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.
- 25.8 The ICT Manager must create a weekly report which lists all of the unapproved change requests, active change requests, cancelled change requests and completed change requests. The report must be reviewed, and actions taken, to ensure that:
- 25.8.1 Change requests receive sufficient attention;
 - 25.8.2 The change control process is being followed for all known changes;
 - 25.8.3 Trends across change requests, that indicate systemic problems in the ICT environment, are identified and require more permanent fixes.

26. HANDLING OF FORENSIC EVIDENCE

- 26.1 Proper handling of digital forensic evidence is crucial to maintaining its integrity and ensuring it can be used effectively in investigations and court proceedings.
- 26.2 The key steps in this process are:

- 26.2.1 Identification of potential digital evidence and documenting its location and condition. It's important to prioritize evidence based on its volatility and value;
- 26.2.2 Collection of digital devices and data systematically. This can involve both static acquisition (collecting data from powered-off devices) and live acquisition (collecting data from running systems);
- 26.2.3 Creating a duplicate copy of the digital evidence without altering the original data. This is done using tools like write blockers to prevent any changes during the copying process;
- 26.2.4 Ensuring that the digital evidence remains unchanged and is stored securely. This includes maintaining a clear chain of custody to document every person who handles the evidence;
- 26.2.5 Conducting a thorough examination of the evidence using forensic tools and techniques. This step should be performed by qualified professionals to ensure the results are reliable;
- 26.2.6 Documenting the findings in a clear and accurate manner, including any limitations or uncertainties in the analysis;

27. BREACH OF POLICY

- 27.1 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 CFO and evaluated on its level of severity.
- 27.2 The appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy.
- 27.3 Actions include, but are not limited to:
 - 27.3.1 Revocation of access to Municipal systems and ICT services;
 - 27.3.2 Disciplinary action in accordance with the Municipal policy; or
 - 27.3.3 Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
 - 27.3.4 Punitive recourse against a service provider in terms of the contract.

28. REVIEW OF POLICY

25.1 The policy shall be reviewed annually.