MORETELE LOCAL MUNICIPALITY

ICT INFORMATION SECURITY POLICY

Policy number	ICT-005-2026
Date of Management engagement	26 June 2026
Resolution Number	13001001-06-2026
Council Approval	30 June 2026
Review Date	26 June 2027
Signature: Municipal Manager	

Change Record

Author	Date	Version	Change
Moretele Municipality	July 2022	1.1	

Reviewers

Names	Date	Version
P.N Mahlo	January 2022	2
R.J Mophuting	January 2022	2

Names	Date	Version
RJ Mophuting	April 2023	3
ICT Steering Committee	April 2023	3

Names	Date	Version
RJ Mophuting	23 June 2026	4
ICT Steering Committee	26 June 2026	4

TABLE OF CONTENTS

GLOSSARY

Asset	Something of value.
Availability	Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
Compliance	Deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.
Computer Equipment	Terminal, any network device, personal computer, notebook, laptop, desktop, docking station, file server etc.
Confidentiality	Protection of sensitive information from unauthorised disclosure.
Data	The representation of facts, concepts, or instructions in a formalised manner suitable for communication, interpretation, or processing by human or by automatic means.
Facilities	Resources to house and support information systems.
Information resources	Include, but are not limited to, all Municipal owned or managed computer and telecommunications hardware, software, storage media, computer logon codes, information transmitted across networks, stored and/or processed by a computer system, printed or written on paper, and spoken in conversations.
Information systems	Manual and programmed procedures. Also known as application systems.
Information	The meaning that is assigned to data by means of the

	conventions applied to those data.
Integrity	Accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
ICT	The scientific, technological and engineering discipline and the management of techniques used in data handling and processing, their applications, computers and their interactions with people and machines, associated social, economic and cultural matters.
MISS	Minimum Information Security Standards that prescribes the security requirements for ALL the State Entities.
Policy	A brief and to the point statement of position indicating intention and direction and enabling decisions.
Procedure	An instruction describing how to achieve the policy or standard.
Technology	Technology covers hardware, operating systems, database management systems, networking, and multimedia.
Virtual Private Network (VPN)	A secured dedicated Wide-Area-Network infrastructure for the business of the Municipality. The Policies of the Municipality applies and documented as the Rules of Access to the VPN.

1. PURPOSE

To communicate policy statement that is aimed at ensuring that only authorized users have timely and appropriate access to computerised information, while safeguarding the information's confidentiality and integrity. This policy ensures that the Municipal ICT security policy attains the following;

- Provide the high level policy for information security at the MLM
- Promote awareness among all employees, contrctors and the consultatnts on the value of information, the risk involved in working with or handling proprietary information and the need to protect information.
- Define the information owners and users responsible for protecting information
- Preserve rights and remedies in the event of security breach.

2. SCOPE

The primary focus of this policy is to ensure protection of the Muinicipality information resources from unauthorised change, destruction, use or disclosure, whether intentional or accidental. All information resources are assets of vital importance to the Municipality, they are critical to the daily operation and to the future advancement of the Municipality.

Information resources include, but are not limited to, all Municipality owned or managed computer and telecommunications hardware, software, storage media, computer logon codes, information transmitted across networks, stored and/or processed by a computer system, printed or written on paper.

This policy relates to all the Municipal information as described above.

2.1 Other related documents

2.1.1 The General ICT General Policy.
2.1.2 The Physical Security Policy.
2.1.3 Minimum Information Security Standards.
2.1.4 Virtual Private Network (VPN) Rules of Access.

3. POLICY

3.1 Development and support of information security processes

ICT and the management of the business units will implement processes to ensure sufficient security, integrity, availability and confidentiality for all the information resources. These processes will address the following issues:

3.1.1 Who has access to information?
3.1.2 The information to which each individual has access.
3.1.3 The obligation of the individual who has access to information to keep it confidential.
3.1.4 The release of information.
3.1.5 The mechanisms to secure information against loss, destruction, tampering, and unauthorised access or use.
3.1.6 ICT General policy will address security issues during the development, purchase and implementation of new information systems. No new system application or network access method will be deployed into production without verification that it meets or exceeds the Municipality's security standards.

3.1.7 The orientation/induction program for new employees will address ICT information security policy. At the time of orientation/induction, each new employee will sign a confidentiality agreement that summarises ICT information security policy and the individual's responsibilities regarding these policy. This agreement will be filed in the employee's records at Human Resources.

3.1.8 ICT function will investigate the misuse of the Munbicipality equipment for private gain.

3.2 Authorisation to Access information resources

3.2.1 Only persons who have valid business reasons for accessing the Municipal information resources will be granted access. Individuals will be given access to information resources in keeping with their job requirements.

3.2.2 No one may access the Municipality information resources or applications without prior written authorisation and approval from the ICT Manager. It is illegal to use any computer or access information stored or maintained by ICT without the proper authorisation and consent of the ICT division.

3.2.3 The new employee access request to the Municipality resources will be completed with all the new employee details including the level of the required access.

3.2.4 The new employee access request form to the Municipality resources will be compiled by Human Resouces, including terminations, transfers, promotions, Interns and contract services.

3.2.5 All passwords to the computer systems are confidential. These include, but are not limited to, passwords to network systems, PCs, voicemail,

applications and Internet. It is a violation of this policy to reveal passwords to anyone without written permission from the ICT division.

3.3 Computer equipment security

3.3.1 Municipality computer equipments may only be utilised for performing business functions. The use of computer equipment for non-business related matters is forbidden. No private files or folders of any nature may be stored on the Municipality computer equipments.

3.3.2 Terminals, network devices, and personal computers in unsecured areas will be secured against theft and use by unauthorised persons.

3.3.3 Personal computers in unsecured areas will be set-up to use power-on passwords, screen-saver passwords and/or keyboard passwords, to prevent unauthorised persons from using the device without providing the appropriate password.

3.3.4 Anyone who signs on to a computer system must sign off and/or physically secure the terminal or PC when leaving it unattended.

3.3.5 Where possible, computer systems will be set up to automatically sign off or password-protect terminals and PCs after a specified period of inactivity.

3.3.6 The hard coding of any password is strictly forbidden. This includes using the "save password" option on any software package if the personal computer is not protected as specified above.

3.3.7 All facilities housing computer equipment must be physically protected from any potential damage. This includes, but is not limited to unauthorised access, sabotage and interference.

3.3.8 Access to computer centre / server room will be secured by means of locked entryways. Only persons authorised to operate or maintain the

computer systems will be issued access cards, or other means for unlocking the entryway. A security authorisation schedule will be established by the ICT division.

3.3.9 A visitors logbook is kept and signed by all personnel that visit the secure area.

3.3.10 Authorised visitors to the computer centre will be escorted by the authorised Municipality or ICT staff, who will accept full responsibility while the visitor is inside any secure area.

3.3.11 Contracted Third Party, Peo Information Technology personnel are granted access to the Municipality resources to fulfill the SLA requirements, howver their activities are subject to similar control and evaluation to that of the Municipality ICT personnel.

3.4 Security of computer-related media

3.4.1 Printed reports containing confidential or sensitive information will be stored in a secure area, inaccessible to unauthorised persons. Confidential reports will be rendered unreadable before being discarded.

3.4.2 Diskettes, tapes, and other media containing confidential information will be labeled "confidential" and will be protected appropriately.

3.4.3 Diskettes, tapes and other medial containing computer files will be stored in areas accessible only by authorised personnel.

3.4.4 Confidential and sensitive business related information will not be left on desks after hours, but must be secured in a safe place, only accessible by authorised personnel.

3.4.5 All external hard-drives containing the Municipality data should be locked and not be accisible by unathorised personnel.

3.5 Protection of computerised files

3.5.1 Business divisions heads and staff members must establish regular schedules for making backup copies of data files stored on personal computers, network file servers, and other computer systems.

3.5.2 Backup copies will be stored in a safe location (not exposed to heat or magnetic fields). Backup copies for network file servers will not be stored in the same room and/or building as the servers or data storage devices.

3.5.3 Disaster recovery strategy has been recommended for all ICT systems and applications. A priority schema, based on risk analysis results, will be maintained and reviewed annually.

3.5.4 Virus protection programs will be installed (current,Forefront) and executed regularly on all computer equipment.

3.5.5 Software will not be copied from public access bulletin boards or other non-ICT computer systems without first being scanned by a virus protection program.

3.5.6 Only licensed software will be used by all employees. All software purchased and used on the Municipal computer equipment is the property of the Municipality. The storage or use of unlicensed software is not allowed.

3.5.7 Passwords will be used where disks, directories, files and other computer resources are shared between users.

3.6 Dial up access to information resources

3.6.1 The Virtual Private Network Rules of Access applies to all dial up access to the Municipal information recources.

3.6.2 The remote dial-up facility provided by the Municipalty will only be used for support purposes. ICT function will only approve after-hours access to the Internet via this dial-up facility once relevant business reasons have been supplied.

3.6.3 Authorised employees, contractors, and other authorised parties will be permitted to use dial-up connections to access the Municipality information resources after work hours, with proper safeguards.

3.6.4 Only authorised Executive members of the Municipality with the permission of the Municipal Manager (MM) or a duly authorized Executive will be permitted to use dedicated, 3G cards to access information resources after work hours or when off-site, with proper safeguards. This measure may also be considered for staff members that are consistently out-of the office also with appropriate permission from the Municipal Manager (MM).

3.6.5 All dial-up connections to the Municipality information resources will be routed through devices that provide for password verification, call-back security, or other similar security features.

3.7 Electronic mail

E-mail is a tool for business communications only, and users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. E-mail communication should follow the same standards expected in written business communications and public meetings.

3.7.1 Ownership

All e-mails created, send or received on the e-mail systems are the property of the Municipality.

3.7.2 Monitoring

The Municipality has the right to assess, monitor and retrieve any e-mail for legitimate business reasons, including without limitation, compliance or non-compliance with this policy.

3.7.3 E-mail use

The following use of the e-mail system is strictly prohibited:

3.7.3.1 The creation and exchange of messages that are offensive, harassing, obscene, pornographic, threatening, inciting violence, propaganda for war or advocating hatred based on race, ethnicity, gender or religion.

3.7.3.2 The exchange of proprietary information, trade secrets or any other privileged, confidential or the Municipality sensitive information. Confidential messages should include a warning regarding accidental transmission to an unintended third party.

3.7.3.3 The creation and exchange of advertisements, solicitations, chain letters and other unsolicited e-mail.

3.7.3.4 The creation and exchange of information in violation of any copyright laws, for example **MUSIC FILES**.

3.7.3.5 Registration to list servers without proper authorisation from ICT department.

3.7.3.6 Messages should not be read or sent from another user's account except under proper authorisation for this arrangement.

3.7.3.7 Altering or copying a message or attachment belonging to another user without the permission of the originator.

3.7.3.8 Users must not compromise the privacy of their password as set out in this policy document below.

3.7.3.9 Address messages to recipients who need to know rather than to everyone you know. Messages sent unnecessarily can impact on the system and user performance.

3.7.3.10 Construct messages professionally (spelling, grammar) and efficiently (subject filed, attachments).

3.7.3.11 Personal use of the cMunicipality e-mail system is not allowed.

3.8 Passwords

3.8.1 Passwords should not be single dictionary words in any language.

3.8.2 The password complexity requirement is always enabled.

3.8.3 Passwords should consist of a minimum of six (6) characters.

3.8.4 The use of telephone numbers or names which can be deduced from information about you, do not constitute a security passwords.

3.8.5 Do not use more than two or more successively repeated characters or numbers in your password.

3.8.6 Expired passwords may not be re-used.

3.8.7 User account is locked after three (3) unsuccessful logon attempts.

3.8.8 Passwords should be changed on a regular basis, at least every 30 days.

3.8.9 The system will prompt users to change their passwords before the expiry of the thirty day period.

3.8.10 Passwords may never be written down.

3.8.11 To prevent the simultaneous compromise of multiple systems, computer users must employ different passwords on each of the systems to which they have been granted access.

3.8.12 All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorised parties.

3.8.13 The hard coding of any password is strictly forbidden. This includes the "save password" option on any software package.

3.8.14 All users are responsible for the security of their username and password and will be held liable for any misuse of resources, where the username and password has been used.

3.8.15 It is therefore imperative that all employees protect their passwords. Disciplinary action will be taken against employees found using other employee's usernames and passwords without approval.

3.9. Secure Web-based information

3.9.1 Users of the Intranet shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system.

3.9.2 Personal information such as home addresses and telephone numbers should remain confidential when communicating on the Internet or Intranet.

3.9.3 Access to web pages should be controlled according to the level of confidentiality of the information and the risk involving access thereto. The implementation of these access control mechanisms should regularly be checked for possible security flaws and questionable risks.

3.9.4 Session encryption should be implemented where knowledge of a user's password during a log-in session to an application over the network is a considerable risk.

3.9.4 Digital certificates should be used where knowledge of a user's password through physical means becomes a considerable risk regarding the confidentiality of the information being dealt with.

3.9.5 Once published, quarterly audits will be conducted on the content to ensure that it has not been corrupted, i.e., the content is current, accurate and remains true to the original requirements.

3.9.6 Intranet information will be securely extended to all employees by providing a controlled and secured centralised point of access to all web-based information.

3.9.7 External customers, i.e. suppliers and trading partners will only be allowed access to the Intranet once a valid business need has been identified and a Third Party Access Agreement has been signed.

3.9.8 Employees will only view information that is appropriate to their position and role within the Municipality.

3.9.9 Due to the possibility of intended malicious activity, browser software will only be downloaded from the Municipality main Intranet web-site.

3.10. Firewall security

Firewalls with intrusion prevention system (IPS) capabilities and predictive threat intelligence shall be deployed to enhance normal system security measures and to prevent advanced persistent threats, advanced evasive techniques, denial of service attacks, malicious code or other traffic that may threaten systems within the network.

Firewalls and or IDS/IPS must also be deployed as appropriate to limit access to systems that host restricted or sensitive information.

Firewalls shall be configured to prohibit by default all traffic that is not explicitly permitted.

Permitted connection(s) and protocol(s) through the firewall must be explicitly defined.

Logical access to the firewalls shall be restricted to authorised employees only. Firewall configuration and log files must be protected against unauthorised access. The firewall shall run on a dedicated machine which performs no other function, and which must at all times be run on the most up-to-date version of the software. All security Incidents shall be logged on the Service Desk tool for mitigation actions.

MLM firewalls routinely prevent users from connecting with certain non-business web sites. Emplyoyees and/or Councillors using MLM computers who discover they have connected with a web site that contains sexsual explicit, racist, violent or other potentially offensive material must immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that usres of MLM systems are permitted to visit that side.

3.11. Multifactor Authenticator

The organization has mandates the use of Multi-Factor Authentication (MFA) for all users accessing its information systems.

MFA shall be enforced for:

- Remote system access
- Privileged or administrative accounts
- Cloud-based services.

The implementation of MFA is to enhance the security of Organizational information systems by requiring the use of Multi-Factor Authentication

(MFA). MFA reduces the risk of unauthorized access and protects sensitive government information in compliance with applicable legislation and cybersecurity frameworks.

3.12. Encryption

3.12.1 Confidental and sensitive documents should be encrypted using a password, the document will only be accessible to both the sender and the recipient.

3.12.2 The sender of the document will forward the password to the recipient of the document by SMS.

3.12.3 The document will only be accessible to the person with the password.

3.12.4 The password should not be shared.

4. VIOLATION OF THE INFORMATION SECURITY POLICY

4.1 Failure to comply with this information security policy will result in disciplinary action in terms of the Human Resources Management prescripts.

4.2 Management in each business division will monitor and counsel their staff in matters of information security.

4.3 The ICT division will perform a monitoring and adherence function. All information related to violations of this policy will be routed to the Municipal Manager for disciplinary action to be considered.

4.4 Access privileges to the information systems will be suspended, pending the outcome of the disciplinary hearing.

5. ROLES AND RESPONSIBILITIES

5.1 Management in each business division will ensure that all ICT policies are addressed at departmental staff meetings at least bi-annually.

5.2 Management in each business division is responsible for determining what information resources its employees need to access in order to complete their job functions, that is, the granting of access to information resources should be commensurate with the employee job responsibilities.

5.3. The Human Resource Management new employee access request form should details all the employee information , access to information resources should be communserate with the employee job responsibilities.

5.3 Management in each business division is responsible for determining which information resources will be made accessible to consultants, contractors, students, and third parties having business relationships with the Municipality.

5.4 It is the responsibility of **each employee** to adhere to this policy.

5.5 Human Resources Management shall ensure that the Municipality employee responsibilities for information security are included in job performance contracts.

5.6 Information security should form part of the new employee induction program and the attendance register should attest as confirmation that the new employee is informed and is aware of the contect of this document.

5.7 This document will be kept relevant and easily accessible by all personnel.

"ANNEXURE A"

6. INFORMATION SECURITY GUIDELINES

6.1 Introduction

The guidelines are designed to familiarise all employees with the basic security principles that must be adhered to, in order to safeguard sensitive information within the Municipality.

6.2 Use and Choice of Passwords

A password provides the means through which access to electronic assets such as sensitive information could be restricted to authorised persons only. For passwords to be effective against human and electronic forms of attacks, composition thereof should include a meaningless combination of a minimum of eight (8) alpha-numeric characters. Poorly constructed passwords, such as dictionary words, pets, friends and family names, date of births, contact numbers, residential addresses, or any word, name or date that is of significance to the user, offer no protection, and thus unacceptable.

Passwords used to log onto the Municipality domain should be unique, in the sense that the password should not be used to access any other electronic assets. Furthermore, users are advised not to reveal passwords, or to type password in the presence of colleagues or strangers. Users should always lock machines [Ctrl + Alt + Delete] when leaving the machine unattended for any length of time.

Users are encouraged to change password regularly, or at least monthly as shall be enforced through policy. Passwords should not be recycled – in other words, password should be used once and only once. No passwords should be written on a piece of paper and affixed to the monitor.

6.3 Antivirus Measures

The anti virus with End Points Detection and Response software is deployed in users' machine to protect all machines against the threat of virus infection, with possible consequences that may results in loss of

electronic assets and possible disruption to daily operations on an organisation wide scale.

Since no antivirus technology offers protection against all conceivable threats, users have the responsibility of ensuring that signature files on machines are up to date, otherwise the machine without the latest signature files are vulnerable to malicious software. A signature file defines the nature and elimination of known viruses.

The  symbol on the system tray indicates that signature files are up to date, and the  indicates that the signature files need to be updated as a matter of urgency.

All users are required to scan machines for malicious software on a daily basis. As a rule, users are advised to run the antivirus software in the morning at 08h00 and at 15h00 and all infected machines should be reported to ICT with immediate effect.

6.4 External Data Storage Media

Sensitive files stored on removable data storage media should be encrypted and password protected, to prevent unauthorised access to confidential information in the event of loss or theft. Users should always dismount and lock into a drawer any external data storage devices connected to machines when leaving the office, even for brief periods of time.

Caution should be exercised to ensure that external data storage media are not interfaced with machines with inadequate virus protection. Consistent with virus protection measures in place, external data storage media should be scanned for virus infection before and after use.

6.5 Internet Access

Since the Internet enables individuals to access information that is relevant to efforts conducted by the Municipality, it is imperative that access to the Internet is construed as a tool with strengths and severe limitations. Thus, owing to limited computer and network resources, users are prohibited from accessing the Internet for personal use, such as conducting shopping online, downloading or uploading sexually explicit material, downloading and installation of unauthorised software, or downloading and transmitting any material that may compromise the integrity of the Municipality.

Users are encouraged to close any open Internet session, once access to the content is no longer necessary.

6.6 Computer Mediated Communication

Electronic communication is one the most convenient form of communication, yet, when such communication medium is not managed carefully, may at best jeopardise the work of the Municipality. Also, since electronic communication may occur without the knowledge or permission of the user, it is always recommended that the intended recipient of the sensitive communication be informed in advance before such communication could be forwarded.

Also, communication of sensitive material should be password protected and encrypted. No user should send communication on another user's machine without explicit permission of the machine owner.

All unsolicited communication should be deleted without opening the message. Communication containing attachments not related to work of

the Municipality should be deleted without opening the attachment, since the execution of attachment may compromise the security of the Municipality.

Chains letters, no matter how well intentioned, and irrespective of religious or cultural significance, are strictly prohibited. Based on sheer volumes, chain letters, when distributed internally or externally, rapidly exhaust available network and computer resources, leading to the denial of service to legitimate users. Moreover, the use of electronic communication to distribute sexually explicit material, recreational content such as humour, unauthorised software and confidential material related to the work of the Municipality to unauthorised person, and advertise private business shall be prohibited.

6.7 Key Logging Devices

While most antivirus solutions are designed to detect and safeguard machines against common software based keystroke loggers, hardware based keystroke logger pose the same threat to confidentiality of sensitive material. In general terms, keystroke loggers, when installed, capture keys input through the keyboard, and screenshots without the knowledge on the users. Through such means, attackers are able to obtain users names and passwords, and thus gain access to sensitive information.

Figure 1

Typical Hardware Keystroke Logger

Figure 2 A Keystroke Logger variant

Figure 1 and 2 above show typical keystroke loggers that resemble innocuous keyboard extension cables. The device may be surreptitiously connected to the target machines by an attacker posing as an air conditioner service person, electrical technician, or a colleague from another office.

For this reason, users are encouraged to be aware of the state of the machine when leaving office for the day, and when using the machine on a daily basis. Users who suspect that the machine may have been compromised should contact ICT immediately.

6.8 Access to Server Room

Access to the server room shall be restricted to ICT personnel, as well as authorised external contractors only including Peo Information Technology personnel. External contractors may only access the server room when accompanied by a permanent ICT personnel.

6.9 Access Control

The ICT systems are used by different staff members, with different access control measures and security requirements. Inappropriate access to a system may cause harm to the information or data hosted in that system. Therefore, access to the systems must be strictly controlled and managed.

6.10 Data and Information

Employees may process personal information or data on personal subjects only if such information is necessary for business purposes and were duly authorised by the relevant authority, or when the privacy subject has given permission that his/her personal information or data be collected.

6.11 Incident Management

The Incident Response Management Process is adequately addressed within the Municipality's existing Incident and Problem Management procedures.

The current framework ensures that all incidents are appropriately identified, reported, managed, and resolved in a structured and timely manner. In addition, problem management procedures provide for root cause analysis and the implementation of corrective actions to prevent recurrence.

6.11 User Privacy

From time to time, remote access to users' machines may be required to, inter alia, deploy new or upgrade software, run software audits, remove unauthorised software, and perform general diagnostic functions such as removal of malicious software from target machines. Users are assured that confidentiality of information on the users' machine would not be compromised in the course of executing such function.

From the ICT perspective, while every effort has been made to protect electronic assets against unauthorised access, users are advised that

such protection cannot be guaranteed when accessing the internet. Even with the best available technology, access to the Internet greatly reduces any privacy protections in place.

6.12 Conclusion

Despite technical controls to safeguard electronic assets of the Municipality, human error may result in loss of confidentiality, integrity and availability of electronic assets. The electronic security guidelines are designed to form the foundation for the conduct and responsibilities of all individuals in respect of protecting confidential electronic assets. Thus, individuals should make an effort to familiarise themselves with these guideline to minimise the risk of human errors.

"ANNEXURE B"

7. ADMINISTRATOR PASSWORD MANAGEMENT PROCEDURES

The procedures detail the minimum standards for system Administrator passwords required to maintain the ICT Services, Facilities and Infrastructure of the Municipality.

7.1 PROCEDURES

7.1.1 The Administrator password for the ICT Services is generated and managed by the ICT Personnel responsible for ICT Services including Infrastructure Management.

7.1.2 Administrator Passwords must be kept secret from any person who is not responsible for the management of an ICT Service and Infrastructure.

7.1.3 All Administrator passwords must meet the following minimum standards in construction:

7.1.3.1 Contain eight (8) characters or more; and

7.1.3.2 Contain characters from the following classes

- Alphabetic (that is: a-z, A-Z);
- Mixture of capitalised and lower case alphabetic characters;
- Numeric (that is: 0-9);
- Special characters such as ?, @, $, %;

7.1.4 Administrator passwords will have a maximum age of six (6) months and will be changed during the closest Administrator windows each system has to February 10 and August 10th of every year.

7.1.5 Administrator passwords must not be used on multiple occasions, and where possible systems should monitor password history;

7.1.6 Upon change of the Administrator password, a new random password should be generated following the rules defined in this Procedure above (point 7.1.3).

7.1.7 Administrator passwords must be kept in a secure, locked place "Strong Room" and accessible only by members of the ICT division who have been appointed as systems administrations.

7.1.8 Administrator passwords must not be stored, or left, in non-secure spaces.

7.1.9 Administrator passwords must be changed if the following events occur:

7.1.9.1 Breach of system, or Administrator account, through external/internal attack, or compromised external connection;

7.1.9.2 Member of the systems administrator team leaves the employ of the Municipality or transfers to another division within the Municipality.

7.1.9.3 Improper storage or handling of the administrator password.

7.1.9.4 Password ageing period has lapsed.

8. REVIEW

This Policy will be reviewed annually to ensure it remains aligned and relevant.

-- END OF DOCUMENT ---