ICT SECURITY MANAGEMENT

APPROVED BY:

MR M NAKO

MUNICIPAL MANAGER

DATE: 17/06/2022

APPROVED BY:

CLLR S JANDA

EXECUTIVE MAYOR

DATE: 17/06/2022

1. POLICY BACKGROUND

Mbhashe Local Municipality needs to reinforce security controls and make sure municipal ICT infrastructure is secured. This policy is to safe guide the municipal ICT infrastructure and detail how to make sure security is enforced.

2. POLICY PURPOSE

The purpose of the ICT Security Policy is to ensure the effective protection and proper usage of the computer systems and its peripherals within the municipality. Each employee is responsible for the security and protection of electronic information resources over which he or she controls. Resources to be protected include, but not limited to networks, computers, software, removable media and data. The physical and logical integrity of these resources must be protected against threats such as viruses, sabotage, unauthorised intrusions, and malicious misuse or in-adverted compromise.

3. DEFINITIONS

ICT: Information Communication Technology

Security: Protection of computer systems from theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the service they provide

Cyber: is a prefix used in a growing number of terms to describe new things that are being made possible by the spread of computers. Anything relating to the internet also falls under cyber category.

4. APPLICATION AND SCOPE

ICT Security Policy is applicable to all employees within the municipality, third parties and stakeholders utilising the municipality's ICT infrastructure and resources in order to fulfil the municipality's goals and objectives

5. LEGISLATIVE FRAMEWORK

The policy is developed with the legislative environment, as well as to leverage internationally recognised ICT standards.

The following legislation, amongst others, are considered in the drafting of this policy:
5.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
5.2 Electronic Communications and Transactions Act, Act No. 25 of 2002;
5.3 Minimum Information Security Standards, as approved by Cabinet in 1996;
5.4 Municipal Finance Management Act, Act No. 56 of 2003;
5.5 Municipal Structures Act, Act No. 117 of 1998;
5.6 Municipal Systems Act, Act No. 32, of 2000;
5.7 Protection of Personal Information Act, Act No. 4 of 2013

The following internationally recognised ICT standards were leveraged in the development of this policy:

5.7 Control Objectives for Information Technology (COBIT) 5, 2012;
5.8 ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls;
5.9 and King Code of Governance Principles

These best practices, standards and legislation form the basis of the structures needed in order to implement the Corporate Governance of ICT

6. POLICY PROCEDURE

6.1 Responsibilities

6.1.1 ICT Manager

The ICT Manager is responsible for overseeing the development and implementation of the Municipality's ICT Security Policy.

In consultation with the Systems Administrator, the ICT Manager shall recommend all ICT improvements of the municipality to the Senior Manager: Corporate Services. Where necessary, a report with recommendations will be submitted to Management.

Ensure that all ICT service providers undergo the necessary security procedures before providing services to the municipality i.e. assessing the credibility and competence of the service provider.

Ensure that Risk Management Policy of the municipality is adhered to in the ICT Unit. Identify mitigating actions to reduce the ICT risks of the municipality to an acceptable level and make recommendations where necessary.

6.1.2 System Administrator

Responsible for overseeing the implementation of the ICT Security Policy.

Maintain and manage relationships with stakeholders and Service Providers by ensuring that all Service Level Agreements entered into are monitored in terms and conditions therein.

Monitor and ensure compliance with relevant ICT Regulatory Framework.

Ensure that all ICT physical security breaches are reported immediately to ICT Manager.

Responsible for physical protection of all ICT assets of the municipality.

In conjunction with Asset Management, ensure that employees are provided with approval to move any ICT assets, other than equipment not registered as assets.

Ensure that the municipality's environment is secured from any internal and external threats.

6.1.3 Internal Audit

Internal Audit shall audit all ICT Compliance within the municipality

Assist ICT Unit in ensuring that recommendations provided from the audit findings are implemented correctly.

7. GENERAL POLICY PROVISIONS

7.1 Third Parties and Contractors

All ICT Service Providers shall be screened before providing services to the municipality to ensure credibility of the service provider.

Sign a non-disclosure of classified information.

A Service Level Agreement must be signed between the municipality and Service Provider before providing any ICT services.

A Service Provider shall not be provided with any logical access to any critical information systems; access will be provided only with approved authorisation from ICT Manager

7.2 Asset Management

All ICT equipment shall be recorded in the Fixed Asset Register and allocated an asset barcode number.

The ICT asset register shall have at least the following descriptive fields:

Asset number, asset owner, location of the asset, category of asset, date of acquisition, asset description and value of the asset.

7.3 Server and Network Room

Servers shall be located in a secure server room that is accessed only by authorised ICT employees.

Service Providers shall not access server rooms without being accompanied by an ICT Unit employee and signing ICT consultant register.

7.4 Patch Management

Patch Management is the responsibility of the Systems Administrator.

The Systems Administrator shall identify patch management resources to update the servers and workstations of the municipality.

Workstations and servers owned by the municipality must have up-to date operating system security patches installed to protect the asset from recognised vulnerabilities. This includes all laptops, desktops, and servers owned and managed by the municipality.

Desktops and laptops must have automatic updates enabled for operating system patches.

This must be the default configuration for all workstations and any exception to the policy must be documented in the Patch Management.

Servers must comply with the minimum baseline requirements. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the municipality asset and the data that resides on the system.

Patches will be tested prior to deployment into the live environment.

7.5 Desktop Security

All desktops provided to employees shall be allocated in accordance with the employee's job description.

Employees shall be given Standard User Access to the desktop operating systems.

Employees shall ensure that they only utilise the equipment for official purposes.

Employees shall only have logical access to their desktop computer.

No employees, except ICT Unit employees are allowed to disassemble or perform repairs to any ICT equipment.

No desktop computers shall be removed from an employee's office without the authorisation of the Systems Administrator and Asset Management.

7.6 Mobile Devices

Mobile devices herein refer to laptops and tablets.

Municipal mobile devices shall be issued to employees in accordance with categories.

All employees issued with municipal laptops must ensure that they are also provided with security cables refer to Security Locking Cable.

It is the employee's responsibility to ensure that the laptop is secured at all times.

7.7 Removable Devices

Removable devices herein refer to USB Flash Drives, Compact and DVD discs, external Hard-drive and any other removable media storage devices.

Removable devices shall be issued to employees as per needs and nature of work.

Any loss of removable devices allocated to an employee must be reported in writing to the ICT unit within 48 hours and Asset Management unit.

7.8 Network Security

Only municipal desktops and mobile devices shall be connected to the municipal local area network, 3rd parties connect with prior approval by Senior Manager: Corporate Services.

7.9 Remote Access

Remote access to Municipal systems is prohibited i.e. Financial System, Payroll System, and other municipal systems.

Only the ICT Manager, Systems Administrator and the IT Technician are permitted to have remote access via Virtual Private Network (VPN).

Remote access will only be granted to an employee in exceptional circumstances with the approval of the departmental HOD's, recommended by Senior Manager: Corporate Services and lastly be approved by Municipal Manager.

3rd party will remote connect with prior approval by IT Manager for any kindly of remote connection with motivation and all signatories.

7.10 Internet and E-mail

Internet and Email will be accessed by employees only approved to have access and approval from HOD's.

7.11 Malicious Software

7.11.1 Definition

Employees are prohibited from installing unauthorised software and software's from untrusted sources.

Malicious software (Virus, Trojans, Worms and Spyware) identified by an employee must be reported immediately to ICT Services Unit. The reporting of the incident is as follows:

i. Contacting the IT helpdesk to report the incident
ii. IT technician shall assist the user to remove the Malicious software
iii. Systems Administrator must ensure that the Antivirus installed on all ICT equipment and setup to scan desktops and servers daily.

Eset Endpoint Protection is currently in use and user computers are updated daily once connected on the internet. Any computer, laptop or other device that is found to be infected with a virus must be attended to immediately and separated.

A record will be kept of all types of malicious software encountered.

7.12 Firewall and Antivirus

It is the responsibility of the Systems Administrator to ensure the effective implementation of firewall and antivirus management for the municipality.

The Systems Administrator is responsible for ensuring that the latest version of antivirus software is installed and signature database is up to-date.

Users of mobile devices should ensure that computers are plugged into the Municipal network at least everyday for antivirus updates.

Employees are prohibited from disabling or interfering with the virus scanning software.

7.13 Incident Management

All the municipal ICT incidents must be reported to the ICT section at helpdesk@mbhashemun.gov.za and copy ICT employees.

ICT incidents shall be prioritised according to the risk and impact they have on the municipal network and critical systems.

ServiceDesk Plus shall be the tool used for logging ICT incidents.

7.14 The Server Security Baseline

Basic Security Step:

Plan the installation and deployment of the operating system and other components for the server.

Install, configure, and secure the underlying Operating System.

Install, configure, and secure the server software.

For servers that host content, such as Web servers (Web pages), File Servers, and Active directory servers, ensure that the content is properly secured. This is highly dependent on the type of server and the type of content, so it is outside the scope of this publication to provide recommendations for content security.

Employ appropriate network protection mechanisms like firewall, packet filtering router, and proxy.

Choosing the mechanisms for a particular situation depends on several factors, including the location of the server's clients (Internet, internal, and remote access), the location of the server on the network, the types of services offered by the server, and the types of threats against the server.

Employ secure administration and maintenance processes, including application of patches and upgrades, monitoring of logs, backups of data and OS, and periodic security testing.

The following items are important to consider, and will make the process of employing security controls more efficient:

Identify the purpose of the server.

Identify the network services and protocols that will be provided on the server examples include HTTP, FTP, SMTP, NFS, and TCP/IP.

Identify any network service software, both client and server to be installed on the server and any other support servers.

Identify the users or categories of users of the server and any support hosts.

Determine the privileges that each category of user will have on the server and support hosts.

Determine how the server will be managed (locally, remotely from the internal network, remotely from external networks).

Decide if and how users will be authenticated and how authentication data will be protected.

Determine how appropriate access to information resources will be enforced.

Determine which server applications meet the organization's requirements.

Consider servers that may offer greater security, even though with less functionality in some instances.

7.15 Server Room Physical Location Considerations

When planning for this location, the following were considered:

Appropriate physical security protection mechanisms for the server and its networking components, including locks, card reader access, biometric scan, security guards, and physical intrusion detection systems like motion sensors, cameras).

Appropriate environmental controls so that the necessary humidity and temperature are maintained, and the possible need for redundant controls.

Backup power sources and how long power can be provided.

Appropriate fire containment equipment that will minimize damage to equipment that would not otherwise be impacted by the fire.

Redundant network connections and redundant data centre locations for high availability systems.

Protection from potential natural disasters that may exist in the server location.

7.16 Strengthening and Securely Configuring the Operating Systems

Remove or disable unnecessary services, applications, and network protocols

The following provide some examples of what services, applications, and protocols that can be removed / disabled if they are not being utilized:

File printer sharing services (Windows Network Basic Input / Output System [NetBIOS] Network File System [NFS], FTP.

Wireless networking services.

Remote control, remote access programs, particularly those that do not strongly encrypt their communications example Telnet.

Directory services like Lightweight Directory Access Protocol [LDAP], Network Information System [NIS]).

7.17 General

All employees provided with ICT equipment must ensure that the ICT equipment is protected from damage and theft at all times.

Any damage to or theft of ICT equipment must be reported writing to ICT unit and Asset Management within 48 hours with case number obtained from SAPS.

Employees not reporting any damage or theft of allocated ICT equipment shall bear the responsibility and the losses recovered from them. This shall be done in compliance with the Asset Management Policy.

8. PROCEDURES FOR IMPLEMENTING POLICY

8.1 Cyber Security

8.1.1 What is cyber security?

Cyber security also referred to as information technology security focuses on protecting computers, network, programs and data from unintended or unauthorized access, change, destruction and misdirection of the service they provide.

8.1.2 What is Cyber-crime?

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming and etc) or is used as a tool to commit an offense.

Cybercriminals may use computer technology to access personal information, communication, data storage, and business trade secrets or use the internet for exploitive or malicious purpose. Criminals who perform these illegal activities are often referred to as hackers.

8.1.3 How Cyber criminals works

Cyber criminals may gain access to secure information in three different ways that is technology, physically or by human shortcomings. Once inside cyber criminals will install malware that will start collecting data. The malware is also and procedure in alignment with natural, daily activities, most employees won't think about the controls unless they are culturally ingrained.

Failure to create adequate control, organisations create controls to minimize activities that could create undue risk. However risks are always changing and not all controls are sustainable, if indeed they were properly created in the first place.

Failure to identify and plan against dynamic risks, threats and vulnerabilities, most risk assessments are a snapshot in time, yet organizations often don't periodically reassess them to identify changes and indicators of adverse events.

8.1.4 ICT Responsibility

Make sure we have right policies in place dealing with cyber security.

Educate employees about cyber threats and defences.

Do our best to stay on top of patching and antivirus updates.

8.1.5 Employee Responsibility

Employees shall not knowingly allow malware to install on municipal computers.

Employees are not permitted to make any changes to firewall settings in their computers.

Employees must not share their personal information using links that looks like competitions or promotions and or employment offers. Suspicious links sent to employees must be reported and need to be verified by IT.

Employees shall maintain control over all devices (Cell phones, laptops and desktops) that belongs to them.

8.2 Code of Conducts

8.2.1 System and network activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use of Mbhashe Local Municipality.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- The Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account and WiFi password to co-workers or none Mbhashe Local Municipality employees or allowing use of your account by co-workers. This includes family and other household members when work is being done at home.
- Using a Mbhashe Local Municipality computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Mbhashe Local Municipality account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not

an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- The deliberate transmission of computer viruses, worms, Trojan software, or other malicious programs.
- Interfering with, disrupting, or denying service including, but not limited to, using any technique to intentionally degrade or disable the delivery of any legitimate data (e.g., denial of service attacks).
- Attempting to gain unauthorized entry to any site or network including but not limited to executing any form of network probing, monitoring or other information-gathering on someone else's site or network.
- Attempting to circumvent host or user authentication or other security measures of any host, network or account.
- Attaching devices to the physical infrastructure of the network without prior authorization from the ICT Unit e.g. personal computer
- Installation of Software without the express permission of the ICT Unit.
- Interference with systems including, but not limited to, removal or change of internal parts.
- Providing confidential information about the Municipality

8.2.2 Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Violates or infringes on the rights of any other person, including the right to privacy.
- Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or illegal.
- Messages that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, or religious or political beliefs.
- Violates municipal or departmental regulations prohibiting sexual harassment.

- Restricts or inhibits other users from using the system or the efficiency of the computer systems.
- Encourages the use of controlled substances or uses the system for the purpose of criminal intent.
- Uses the system for any other illegal purpose.
- Conduct any non-approved business.
- Solicit the performance of any activity that is prohibited by law.
- Transmit material, information, or software in violation of any municipal law.
- Conduct any non-governmental-related fund raising or public relations activities.
- Engage in any activity for personal gain.
- Make any unauthorized purchases
- Unauthorised use, or forging, of email header information or Signature.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, who were not previous customers or with whom the sender did not have an existing business relationship ("E-mail spam").
- Harassment including, but not limited to, through language, frequency or size of messages.
- Unauthorized use, or forging, of mail header information.
- Solicitations of mail for any other E-mail address other than of the poster's account or service with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or other "schemes" of any type.
- Mbhashe Local Municipality also reserves the right to monitor any content that passes through the mail system as well as enforcing content filtering mechanisms that are deemed necessary.
- Because electronic messages are typically stored in one place and then forwarded to one or more locations, often without the specific knowledge of the originator, they are vulnerable to interception or unintended use. The Municipality will attempt to provide an electronic messaging environment, which provides data confidentiality and integrity. The Municipality cannot be responsible for web-based e-mail systems, however, such as Yahoo, Gmail, etc. Municipal employees should always be aware of the risks.
- Use of unsolicited E-mail

8.3 Blogging

(A blog is a discussion or informational website published on the World Wide Web consisting of discrete, often informal diary-style text entries or posts. Posts are typically displayed in reverse chronological order, so that the most recent post appears first, at the top of the web page.)

Blogging by employees, whether using municipal property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Code of Conduct. Limited and occasional use of municipal systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Mbhashe Local Municipality Code of Conduct, is not detrimental to municipal best interests, and does not interfere with an employee's regular work duties. Blogging from municipal systems is also subject to monitoring.

Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Mbhashe Local Municipality and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

Employees may also not attribute personal statements, opinions or beliefs to the municipality when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Mbhashe Local Municipality. Employees assume any and all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Mbhashe Local Municipality trademarks, logos and any other Mbhashe Local Municipality intellectual property may also not be used in connection with any blogging activity

8.4 Internet

All private use of Municipalities Internet / E-mail systems must occur outside normal working hours and may not be to the prejudice of the Municipality. The same standards of conduct apply to employees for personal use as that set out for Municipal use. Employees should note that they are directly and personally liable and responsible for any obligations, illegal activities, commitments, undertakings, or any other abuses that may occur.

All employees who use the Internet / E-mail for personal use shall indemnify and hold the Municipality harmless against all claims, losses and costs the Municipality may become liable for by reason of such use and hereby authorize the Municipality to make deductions from and to retain from wages any amount necessary to entirely discharge this liability.

Internet access provides necessary access to information for many municipal employees. Employees are responsible for making sure they use this access correctly and wisely.

Inappropriate uses of the Internet include, but are not limited to:

1. Viewing, downloading or sending pornographic materials.
2. Visiting and/or participating in chat rooms not designed for professional interactions specifically related to one's job.
3. "Surfing" the Web for inordinate amounts of time.
4. Otherwise endangering productivity or the Municipality.

Such matters will be interpreted as gross misconduct.

8.5 General Rules

8.5.1 Internet user indemnity

- Only I shall have access to my Internet name and password and will not hand it out to anyone except my supervisor. Should I give my password to anyone else, I will still be held responsible for my Internet account.
- I will log out of Internet, if the workstation is unattended for a period of time.
- I will not abuse my Internet account by accessing sites which are deemed indecent or insulting.
- I will not download material that has no relation to my job function.
- I will not download anything of a pornographic nature.
- I will not download or install any illegal software
- I will only use my Internet for company sanctioned business reasons.
- Limited personal use of the Internet is permitted'. However, if this facility is abused, or is conflicting to any of the other rules it will be revoked!
- I understand that my Internet usage will be monitored as part of normal systems administration.

It should be understood that if the above is not adhered to, disciplinary action can be taken, up to and including dismissal.

8.5.2 Network User Protection

General Username and Password Rules:

- I undertake to guard the confidentiality of the information to which I will be granted access, by adhering to the following rules:
- Only I shall have access to my Username and Password and will not divulge it to anyone nor shall I write down my Password and leave it where the security thereof may be compromised.
- Should I divulge or inadvertently compromise the security of my Username and Password, I understand that I will be held responsible for all transactions performed on my workstation with my allocated Username.
- I shall ensure that my workstation is logged out of the network system or locked when unattended for a period of time.
- I shall change my Password as and when prompted to do so by the system.
- I shall conform to the standards set in the Strong Password Security
- I shall, at all times, take good care of my workstation as it is a valuable company asset and report any problem(s) on the call logging system at
- I undertake not to download or install, any unauthorized applications, unless cleared with the Systems Administrator.
- I will not make copies of any software and/or data and remove it from the premises without prior arrangement with the Systems Administrator.
- If I store (data) information on my hard drive, I am responsible for backups of the data or I will make arrangements with the ICT Unit to do so periodically.
- I understand that the content of my network drives will be monitored as part of normal system administration.

- I understand that the remote control feature may be used from time to time in the process of end user support, computer asset control and network problem solving.
- It should be understood that if the above is not adhered to, disciplinary action can be taken, up to and including dismissal.

8.6 Password security

8.6.1 Password standards

- Different levels of password security, if appropriate, will be created for users and accounts with differing levels of access and authorisation where applicable.
- All user-level passwords (e.g. email, web, computers, financial system, HR & Payroll system, etc.) must be changed at least once **every thirty (30) days**.
- All **system-level passwords** (e.g. admin, administrator, application administration accounts, etc.) must be changed at least every six (6) months.
- The password security on the system has been set in such a way that it automatically **disallows familiar passwords.**
- The windows system has been set such that it automatically logs off users if there are more **than five minutes** of inactivity on the station i.e. auto log off.
- Many login attempts will lock the user account temporally or be unlocked by System Administrator.

8.6.2 Password protection

It is the responsibility of account holders to make sure that their accounts are secure at all times. Users must make sure that their accounts are closed either when not using them or when they have to temporarily attend to something else. Any fraudulent, malicious, damaging and destructive activity to the department that is conducted through a user's account due to negligence will attract disciplinary action in line with the Public Service Disciplinary Code.

- Users should not use the same password for municipal accounts as for other non-municipal related accounts (e.g. your private phone account) As much as possible, do not use the same password for multiple municipal accounts.
- Users should not share their municipal passwords with anyone for any reason at any time (secret password). If someone demands a password, refer them to this document or have them contact the IT Manager. Even IT technical staff may not demand a password even if they are assisting with technical issues, but can only ask the user to enter his/her password.
- Users should not permanently store passwords on any file (written or electronic) including e-mail messages, palm pilots or similar devices (unless encrypted according to the Acceptable Encryption Policy).
- If an account or password is suspected to have been compromised, the user is responsible to ensure that the case is reported to IT.
- If user or employee contract terminated, password or account will be terminated within 24 hours once ICT office is made aware by HR office.

8.6.3 Password guidelines

The following guidelines are provided to be used when creating a password:

- Choose a password of eight(8) or more characters in length
- Choose a password that contains a combination of the following:
- a-z (lower case alphabetic characters)
- A-Z (upper case alphabetical characters)
- 0-9 (digits)
- @#%_-+=:,. (special characters)
- Choose a password with at least (1) digit
- Choose a password that does not need to be written down to remember
- Choose a password that can be typed quickly (especially) if account is used in public access areas like labs or public access terminals)
- Think of an easy to remember phrase, such as "**it's Easy to Create Good Passwords!.** From this phrase extract the first letters and special characters. Also substitute the number 2 in the place of the word "to" and vary the case of the letters. This methodology leads to a password of **"I'se2CgP"**
- In all cases, please abstain from:
- Choosing a password that has the title of a movie, book, or composition
- Choosing a password that has any mythological or fictional character or race
- Choosing a password those results from patterns on the keyboard
- Choosing a password that has many repeating characters
- Choosing a password that you have used previously
- Choosing a password by applying a simple algorithm against previous passwords

Examples of good passwords

Password	Source	Phrase
2WeWee, WipkNH!	Church song	Wandikhupha emgxobhozweni Wandibek"endawen'ebanzi; Wafak'ingoma phakathi kwam, Ndiyavuma" Haleluya!
M5:8Batpih4twsG	Bible verse	"Mathew 5:8 Blessed are the pure in heart:for they will see God"
5tltbb &eL	phrase	"Five times I travel between Bisho and East London"
F1, daPitbttehtm	phrase	"For once, driving a Pajero is the best thing that ever happened to me"

Examples of bad passwords

Password	Source
Madikiza7	Based on the user's name, no special character
PORSCHE911	Proper name, in the dictionary, no special character
Qwerty_ui	Letter series based on keyboard
Mhlekazi	Common word in Xhosa
June2007	Name of month, too obvious
Password@1	Password

8.7 Responsibility for Implementation

The Municipal Manager has the responsibility and authority to origin this policy to be implemented and maintained in the Municipality.

8.8 Enforcement of this policy

Any user found to have negligently violated this policy, or the supporting standards and guidelines, may be subject to loss of certain privileges or services including, but not necessarily limited to, the loss of network services, department disciplinary actions up to and including termination of employment, as well as possible civil and criminal cases in a court of law.

9. IMPLEMENTATION

2022/2023

10. REVIEWAL

Annually