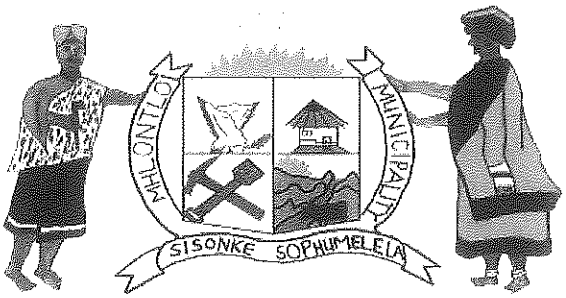


MHLONTLO LOCAL MUNICIPALITY CORPORATE INTEGRATED ICT POLICIES

Financial Year: 2019 - 2020

Contents

SECTION ONE

POLICY STATEMENT, OBJECTIVE, SCOPE & POLICY APPROACH

---

1. SECTION 1: POLICY STATEMENT

1.1 Introduction

The Information and Communications Technology and Security policy is a formal statement of the rules and guidelines applied by the Municipality which must be adhered to by people utilising and managing the ICT facilities. This policy has been developed in line with the Electronic Communication Security Act, 68 of 2002, the South African Minimum Information Security Standards, and Control Objectives for Information Related Technology (COBIT), ISO 17799, System Administration, Networking and Security Institute (SANS) and Information Technology Infrastructure Library (ITIL).

1.2 Objective

The purpose of this policy is to formalise an Information and Communications Technology (ICT) Usage and Security Policy, which provides guidelines for introducing and maintaining ICT into the Municipality in a controlled and informed manner, while addressing the key elements of control and security. Those who use the Municipalities ICT facilities are expected to do so responsibly and within normal standards of professional and personal courtesy and conduct.

The purpose of this policy is:

1. To inform users and managers of their responsibilities when utilising information assets, as well as for protecting technology and information assets;
2. To specify the mechanisms through which these requirements must be met
3. To provide a baseline from which to acquire, configure and audit computer systems and networks in compliance with the policy;
4. To minimise disruption to and misuse of the municipalities ICT infrastructure;
5. To ensure that the municipality's resources are used for purposes appropriate to the business mission; and
6. To define what users may or may not do on the various components of the system infrastructure.

Users are hereby informed of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of this policy will result in disciplinary action in line with the Municipality's disciplinary code.

1.3 Scope

The policy applies to:

1. All ICT infrastructure and systems owned and or used by the Municipality
2. All electronic communications systems and services provided by the Municipality or through third party ICT service providers
3. All users who authenticate to the Municipality's infrastructure, systems and ICT facilities
4. All records and data in the possession of the employees or other users

The policy deals with the following domains of security:

1. Management of Information Security;
2. Management and Protection of ICT Infrastructure and Electronic communication;
3. Asset Management Physical Security and Environmental Controls;
4. System Acquisition development and maintenance;
5. Management of Human Resource Security and System Access;
6. Business Continuity Management;
7. Management of Third Party Relationships;
8. General Usage and Controls of ICT Services; and
9. ICT Risk Management.

1.4 Policy Management & Approach

In order to document a comprehensive ICT policy, all aspects of ICT must be considered and clear rules and guidelines recorded which are appropriate to the culture and risk profile of the Municipality. To define a security policy, a threat analysis must be completed. This is a process where all possible threats to a system are identified and the severity of each threat is measured. This forms the basis of the security policy. Thereafter, once the security policy has been defined, it must be used to decide what security measures must be selected. These are the basic mechanisms used to implement security in a system or organisation.

This document, together with the following documents, forms the basis of the ICT documentation of the Municipality:

1. Disaster Recovery Plan - DRP
2. ICT Governance Framework
3. Backup Procedures
4. Network Diagrams
5. SA Minimum Information Security Standards
6. COMSEC Act 68 of 2002
7. IT Strategy

1.5 Policy APPROVAL AND AMENDMENT

Approval of this policy is vested with the Council. Advice and opinions on the policy will be given by:

1. IT Steering Committee
2. Internal Audit
3. External Audit

Formulation and maintenance of the policy is the responsibility of the Municipality's ICT Unit and the Head of Department under which ICT is aligned to, Awareness of the content and application thereof is the responsibility of the Management of the Municipality.

The ICT Unit will be the custodian of all strategic system platforms, communication systems and central computing facilities. The nominated system owners of each Department will be the custodians of the strategic application systems under their control, while every user will be the custodian of the desktop systems and equipment under their control.

1.6 Policy Revision

Information technology is a fast growing industry with rapid changes and as such this policy shall be reviewed annually to accommodate the variances. Any amendments to this policy must be submitted to the ICT steering committee by the head of departments. The ICT Unit will affect the necessary changes and the policy will be approved in terms of the Municipality's policy approval process.

1.7 Applicability

This policy applies to all councillors and officials including third-party agents, temporary, contract staff and anyone who comes into contact with the council's resources, sites, properties that fall under the operational jurisdiction of the authority, council information or information systems. It also applies to all current locations, and new locations shall take the policy into account during the design, development or feasibility of access control systems being installed in new computing equipment or as part of any major or minor improvement project.

The above will be referred to as users in the rest of this document.

1.8 Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action.

1.9 Terminology

Municipality shall mean Mhlontlo Local Municipality (MLM).

ICT shall mean Information and Communication Technology.

User shall have been anyone who connects 'to or used MLM ICT services.

Policy shall mean this policy.

SECTION TWO

INFORMATION SECURITY

---

2. SECTION 2: Information systems Security

2.1 Overview

The COMSEC (Communications Security) Proprietary Act and various International Standards and Guidelines requires organisations to develop and implement their Information Systems Security policies to safe guide their data and information systems. This Policy has been developed by the Municipality to conform to the Minimum Information Systems Security Standards of South Africa and to protect the Municipality's ICT assets and Data. This policy also serves as a guideline for users to follow when using the ICT infrastructure so as to minimise the risk of errors, fraud and loss of data, confidentiality, integrity and availability.

The policy covers the following minimum requirements:

1. Information Security Responsibilities
2. Classification of Information Sensitivity
3. Access Control
4. Management of Fixed Password
5. Confidentiality
6. Third Party Disclosure
7. Acceptable Use of the Internet
8. Encryption
9. Electronic Mail
10. Printing, copying and fax transmission
11. Mobile computing and working from home
12. Viruses, malicious software and change control
13. Personal use of information systems
14. Intellectual property rights
15. System Development
16. Reporting problems
17. Non-compliance situations
18. Disciplinary Measures

2.2 Information Security responsibilities

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

2.2.1 ICT Steering Committee

ICT Steering Committee charter shall be developed to define a mandate for the establishment of the ICT Steering committee.

Members of the ICT Steering Committee shall also be members of the Change Management Committee and Disaster Recovery Committee.

An ICT Steering Committee shall meet according to the requirements of the ICT Steering Committee Charter to fulfil responsibilities defined therein.

2.2.2 Information Owners

The application and data owner's responsibility shall be delegated to the head of that department and their responsibly shall be as follows;

1. Assign application access rights to existing users and groups within the application.
2. Authorize user removal form.
3. Keep the application administrator passwords in a secure environment.

2.2.3 Custodian of Information

The custodianship of the information shall be dedicated to the information Technology department. Their responsibility shall be:

1. To ensure that all appropriate personnel are aware of and comply with this policy.
2. To create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

2.2.4 Information Users

Users will at all times adhere to the Information Security Policy, report all deviations thereof to the Information Security Officer and use the available infrastructure for business purposes only.

2.2.4.1 Information Security Section

The duly appointed security officer/information security section provides corporate governance and strategic alliance and empowers ICT STEERING COMMITTEE to enforce this Information Security Policy.

2.2.5 Internal Audit Section

The internal section shall conduct regular security audits in line with ISO 17799 checklist and submit reports to the ICT steering committee for deliberation and action

2.2.6 Employee Responsibility

All Councillors and employees must ensure that all reasonable precautions are taken to protect business critical data against unauthorized access, especially data on laptops and portable data storage devices. A locked car in a public area is not a reasonable precaution. It will be the sole responsibility of the user to backup and maintain security of non-municipality critical data.

2.3 Classification of Information Sensitivity

2.3.1 Reasons for Classification

Information needs to be classified in order to conform to the Protection of Private information act and in terms of the Promotion of Access to information Act. The MISS also ISO 17799 further promote the classification of information so that the municipality can be in a position to understand information assets it holds and manage their security appropriately.

2.3.2 Default Category

Information shall be classified in terms of SECTION 6 of the Protection of Private Information Act, and the following default classification levels shall apply;

1. Public
2. Private
3. Confidential
4. Secret
5. Top Secret

Classifications shall also be detailed in the municipality's records and archive policy

2.3.3 Labelling

Documents shall be labelled in terms of SECTION 4 Paragraph 1 of the Minimum Information Security Standards of South Africa.

2.3.4 Handling Instructions

Documents shall be handled in terms of SECTION 4 Paragraph 3 to 17 of the Minimum Information Security Standards of South Africa.

2.4 Access Control

Access Control is essential to create an optimal information security environment. In terms of the Control of Access to Public Premises Act (Act 53 of 1985) the Municipal Manager (Head of state Organ) is responsible for safeguarding the premises used by or under the Municipality.

2.4.1 Access Philosophy

The Municipality from time to time deals with members of the public, business people and other Government workers and foreigners. In order to protect the Municipality against unauthorised access to the premises all areas within the back office environment are in a restricted zone. Areas in the demilitarized zone shall be accessed during working hours.

2.4.2 Access Approval Process

Anyone requiring access to the Municipal Premises shall do so by completing a form and submitting the designated Security Officer who will then confirm with the respective Official whether or not to grant access to the person applying for access to the premises. A register shall be kept at all access points exposed to the public of Visitors and vehicles accessing the Municipal Premises.

2.4.3 Default Facilities

The Municipal Facilities shall be classified as follows:

1. Demilitarized Zone – public areas
2. Restricted Access – areas accessed by staff members or by approval
3. Authorised Access Only- specialised access only

2.4.4 Departure from the municipality

Any Visitor who has been granted access shall sign the visitors register in which they will indicate the date and time departed. All visitors' tags shall be returned to the Security Officer upon Departure.

2.4.5 Unique user ID's

Every user shall be given a unique user id and password to access the network and an access tag to access the premises.

2.4.6 Privileges Deactivation

By default, all users shall be deactivated from administrator privileges on the network and on their workstation. Access to information systems and other ICT services shall also be deactivating by default and only given to the user once the relevant approvals have been made.

2.4.7 User Authentication

Windows active directory shall be used to manage all user authentications to the domain; every user shall be forced to join the domain and shall only work on the network if they are authenticated. Any user who fails to follow this protocol and or bypasses the system security shall be taken to a disciplinary enquiry.

2.4.8 Segregation of Duties

The municipality's systems and technical support staff must support a clear separation of functions (such as ICT Systems Officers vs. regular users) to prevent unauthorised access and functions being performed.

The General Managers must determine and establish the IT user roles and responsibilities in their department to ensure that IT Unit can adequately enforce segregation of duties.

Segregation of duties (SoD) must be practiced to ensure that no single individual has the authority to execute multiple conflicting tasks with potential to impact other systems or information; and that no single individual can execute conflicting end-to-end transactions.

2.4.9 Remote Access Software (RAS)

Remote access shall be granted to users at the sole discretion of MLM and on the terms and conditions that the municipality may determine from time to time.

Remote access to MLM's computer systems from outside the premises shall only be attempted by way of remote facilities provided by MLM utilising the remote access procedures.

2.4.10 Third Party Access

At the end of the contract, the third party must return or destroy all municipal technical connectivity information at the external site and all third party access rights to the municipality's IT assets must be removed.

2.5 Management of fixed password

2.5.1 Creating Passwords

The responsibility of creating passwords for all users in the Network is limited to only the Information Security Administrator, these passwords are not be accessed by anyone in the municipality unless authorised by the Municipal Manager with the supporting documentation.

2.5.2 Changing Passwords

Users must change passwords after every 2 months. If a user has forgotten his/her password or if the password expires then the user must request the Information Technology Department to change his/her password by completing the relevant forms and submitting them to the ICT Unit. Passwords for the members of Council are set not to expire, this is because their computers do not connect to Municipal Network on a daily basis.

2.5.3 Protecting Passwords

Users are strictly prohibited from sharing passwords and it is their duty to ensure that the passwords are unique and are protected from other users. Passwords are not to be written or said out loud.

2.5.4 2.5.4 Dormant Accounts

Officials/users - Password set not to expire and Manual change every 3 months

Members of Council – Password set not to expire and manual change every 6 months

2.6 Confidentiality

The privacy policy defines reasonable expectations of privacy regarding issues such as monitoring of email, recording of keystrokes and access to users' files. Data confidentiality is mandated by law, and different classes of information warrant different degrees of confidentiality. Audit data may contain personal information, and searching this data could represent an invasion of privacy.

The Municipality owns the computers, networks, systems and data that comprise the information technology infrastructure. The electronic allocation of file space to a user does not assign legal ownership of the content; rather it is the granting of permission to use these facilities subject to the policies and regulations of the Council.

All data stored on the Council's systems remains the property of the Municipality, and may be subject to disclosure or inspection at any time. The Municipality does not accept any responsibility for the privacy, security or confidentiality of data or information held on the Council's ICT facilities. Users are responsible for the integrity of all data, and must protect Council data from unauthorised access. At any time and without prior notice, the Municipality management reserves the right to examine email, personal files and other information stored on its equipment.

2.7 Third Party Disclosures

The Municipality does not hold itself accountable to any action of the employee which are done out of this policy all emails and communication to the public shall be sent out with a disclaimer. Only information communication from the municipal manager shall be considered as official and binding to the municipality.

All IT service providers are identified, managed and monitored in accordance with service level agreements. Contracts exist to formalise all key relationships with current IT service providers for IT hardware and software maintenance, networks, telephony, etc. These contracts should include the following:

1. Minimum required service levels
2. Key performance indicators (KPIs)
3. Requirements for monthly performance reporting from service providers
4. Penalties for contract violation or non-performance.

2.8 Acceptable Use of the Internet and Email

Internet and email usage is not a fringe benefit and information obtained from the internet can be confirmed as reliable. Acceptable usage shall be determined by SECTION's 4 and 5 of the Information & Communication Technology Usage and Security Policy.

2.9 Encryption

A certificate server shall be installed for encrypting and decrypting data over the Network, encryption will be used when accessing the network remotely via VPN

or Web Access. All data classified as confidential, secret and top secret shall be password protected and encrypted if sent over electronic mail.

2.10 Printing Copying and Fax Transmission

Printing, Copying and Faxing of classified information shall be conducted in terms SECTIONs 4 and 5 of the Minimum Information Security Standard (MISS).

All waste copies shall be shredded and must not be left lying around in public areas. The following precautions must be taken when faxing, copying or printing information;

1. Password protect, Private, Confidential, secret and top secret documents.
2. Remove all documents from the printer, copier or fax after transmission
3. Clear the devise memory to prevent reprinting
4. Delete all documents in the memory if the device is taken in for repairs
5. Use a register to control incoming and out coming faxes

2.11 Mobile Computing and Working at Home

Any user requiring remote access into the network must be authorised by the Municipal Manager, Remote access shall be location independent for wireless connection however such access will be restricted via password authentication or VPN client authentication.

The municipality shall provide the following remote access control options;

1. Direct access via the VPN through Telkom line (Remote sites, Management, ICT)
2. Remote Access via wireless, Dually authorised 3G card users
3. Web Access (Any user with an email address and Active Domain Account)
4. Push and Pull Access (Users with handheld devices requiring synchronisation of Emails)

Users are responsible for the safe keeping of municipal equipment and are therefore expected to ensure that the equipment is not stolen or damaged whilst in their care, should the equipment be stolen or damaged due to negligence and or failure to follow this policy that user will be held liable for replacement costs.

Any loss or damage must be reported in terms of the Municipalities asset management policy.

2.12 Viruses, Malicious Software and Change Control

The Municipality has deployed an antivirus utility to protect its assets against viruses, Trojans, worms and other malicious software which may damage its data and information systems. The ICT Unit will schedule regular antivirus and software updates to reduce vulnerabilities in the network, users must therefore ensure that they authenticate daily and may not make any changes to configuration settings.

Users are prohibited from disabling; cancelling or deleting any antivirus or software installed by the ICT Unit on Municipal ICT equipment and may not change any configuration setting on their computers.

ICT will notify users in advance via email or system notification if there is an upgrade or replacement of the antivirus software or updates to the firmware and software.

2.13 Security Log Management (Audit log review)

Logging must be designed to record breaches, anomalies and unauthorised actions as well as compliance with security policies and practices.

Selected critical municipality applications must be supported by logs that allow system activities to be recovered.

Changes to the system environment made by privileged access must be logged, particularly where those resources are not normally changed during standard operation.

Log collection must not endanger either network bandwidth availability or system performance.

System logs must be securely transmitted and collected, protected and appropriately archived. All logging information must be maintained in a form that cannot be readily viewed or modified by unauthorised persons. The interruption or corruption of log data must raise an alert and itself be recorded in independent logs.

Secure Retention of Logs: Logs must be retained for at least one (1) month and archived for no longer than one (1) year. During this period, logs must be secured so they cannot be modified, and can be read only by authorised persons.

To allow proper remedial action to be taken in a timely manner, records reflecting security-relevant events must be periodically reviewed by IT staff and escalated to the General Manager – Corporate Services and/or IT Steering Committee.

Computer clocks must be synchronized to ensure the accuracy of audit logs for investigations or as evidence in legal or disciplinary cases. Computers and communication devices that have the ability to operate as real-time clocks should be set to an agreed standard.

2.14 Personal Use of Information Systems

Municipal information systems and equipment are issued to users for official use only, users are prohibited from using Municipal Equipment for personal use and cannot be used by anyone who is not employed or contracted to the Municipality.

Only the ICT Unit is allowed to test software on Municipal ICT infrastructure.

2.15 Intellectual Property Rights

Notwithstanding the provisions of any other law, all intellectual property rights in any product, service, item or any other thing relating to the municipalities technology or systems developed, designed or invented for usage by the municipality or its employees, vest in the municipality.

The Municipality shall direct how the product, service, Item or any other thing relating to the municipalities technology is utilised.

Users are prohibited from making copies of any software or data without authorisation from the Municipal Manager. The ICT Unit may make copies of any original software for backup purposes only.

2.16 System Development

System development and or procurement shall be done in terms of this policy

2.17 Reporting Problems

Incidents shall be managed in terms of this policy.

2.18 Non-Compliance

Should a user fail to comply with this policy disciplinary action must be taken in terms of the municipality's disciplinary code of conduct.

2.19 Change Management

Every change to Mhlontlo Local Municipality's production information resources is subject to the Change Management Policy and must follow the approved Mhlontlo Local Municipality's Change Management Procedure Manual. (Addresses COBIT Control Objective AI6.1)

A risk assessment level will be associated with every change and will be assigned using the predetermined criteria. Prior to migration to production, changes are authorised by the appropriate stakeholder. The approving authority will be based on the risk assessment. (Addresses COBIT Control Objective AI6.2)

Procedures must exist to govern emergency changes to information systems and related technology. Criteria that define an emergency change must be clearly documented and communicated. Emergency changes must be documented. Emergency changes must be approved by a member of ICT management authorised to approve emergency changes. (Addresses COBIT Control Objective AI6.3)

Vendor developments or modification must be governed by an approved system development methodology outlined in the service level agreements.

Emergency changes, that bypass some of the elements of the established change control system, may need to be performed. Such actions require the authorisation of all affected departmentses and acknowledgment of the risks involved. Such actions must be controlled, logged, restored and be kept to a minimum.

The development of new application or system software should be kept; both physically and logically, separate from the production environment. The

development staff should not normally have access to production systems. For occasional and essential support purposes, the development staff may be granted special access for a limited period of time (e.g., by issuing secure passwords via an emergency access process).

A system must be in place to support the recording and tracking of changes made to information systems. If customer notification is required, it must be completed for each change following the steps contained in Mhlontlo Local Municipality's Change Management Procedure Manual. (Addresses COBIT Control Objective AI6.4)

Technical and user documentation must be updated to reflect changes made to information systems and related technology. A process must be defined for reviewing changes to ensure successful implementation. (Addresses COBIT Control Objective AI6.5)

A central repository must exist to contain all relevant information on configuration items. This repository includes hardware, application software, middleware, parameters, documentation, procedures and tools for operating, accessing and using the systems and services. (Addresses COBIT Control Objective DS9.1)

SECTION THREE

INTERNET USAGE

---

3. SECTION 3: internet usage

3.1 Overview

The Municipality provides its employees access to the vast information resources of the Internet with the intention of increasing productivity and achieving service delivery excellence through knowledge and sharing of best practises with other Municipalities. While the facility has the potential to help you do your job faster or smarter, there is justifiable concern that it can also be misused. Such misuse can waste time and potentially violate laws, ordinances, or other policies. This Internet usage policy is designed to help you understand the expectations for the use of these resources.

The underlying philosophy of this policy is that Internet access from the Municipality is primarily for municipality related purposes including communicating with service providers, suppliers, colleagues, to research relevant topics and to obtain useful business information. In addition, all existing laws and municipal policies apply to your conduct on the Internet, especially those that deal with intellectual property protection, privacy, and misuse of municipal resources, sexual harassment, data security, and confidentiality.

The policy covers the following domains;

1. Employee responsibilities
2. Restrictions
3. Non Restrictions
4. Standard Internet/Email Practises
5. Acceptable use of the Internet
6. Unacceptable Use of the Internet
7. Posting of Information to information Groups
8. Downloading of Software
9. Sending of Security Parameters
10. International Transfer of Data
11. Setting up of Extra Services
12. User Anonymity

13. False security reports
14. Establishment of Network Connections
15. Dial up Access
16. Third Party Access

3.2 Employee Responsibility

The display of any kind of obscene image or document on any Municipality's computing resource may be a violation of existing Municipal policy on sexual harassment. In addition, obscene material may not be archived, stored, distributed, edited, or recorded using Municipal network, printing, or computing resources.

No employee may use Municipal facilities to download or distribute pirated software or data. Any software or files downloaded via the Internet may be used only in ways that are consistent with their licenses or copyrights. All requests for file downloads must first be authorised by the IT Unit.

No employee may use the Municipality's Internet facilities to propagate any virus, worm, Trojan horse, trap-door, or back-door program code or disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.

The Municipal Internet facilities and computing resources must not be used to violate the laws and regulations of South Africa or any other nation, or the laws and regulations of any state, Federation, province, or local jurisdiction in any material way.

Each Municipal employee using the Municipality's Internet facility shall identify themselves honestly, accurately, and completely when corresponding or participating in interactive activities, and shall not send unsolicited mass electronic mail.

Employees should not assume that any Municipal data or databases are subject to any Transparency Laws, but rather bound by the Code of Secrecy. There are numerous exclusions to these laws and such data or databases may not be uploaded or otherwise transferred to non-Municipal entities without appropriate approvals.

Employees should not have any expectation of privacy as to his or her Internet usage.

Municipal Internet Usage and Email Usage will be monitored and the Municipality shall reserve the right to check any internet or email content sent via its network.

Municipal employees are not allowed to change the internet settings set by the Municipality's ICT Unit.

3.3 Restrictions

The Municipality reserves the right to grant, deny or restrict access to any website, facility, and email size and network bandwidth. The internet activities are prohibited however it is not limited to the following:

1. Downloading of files e.g. MP3, MPEG, EXE, WAV & other malicious Software
2. Access to social sites e.g. Face book, MySpace or any other chat sites
3. Accessing Pornography Sites.
4. Downloading pirated software to be installed on Municipal Computers.
5. Accessing music sites

3.4 Non Restrictions

The Municipality shall declare the following sites as non-restricted and users shall be granted access to these site however the Municipality still reserves to right to restrict these should it deem it necessary to prevent abuse.

1. Online Banking
2. Government websites
3. Medical Aid sites
4. Academic website
5. Municipal Web site
6. Municipality's intranet and internet webpage

3.5 Acceptable Use of the Internet

Internet is a cost efficient and effective research tool which is provided to Municipal Employees for Business usage only. This tool can also be used to surf for pornography, adult material, downloading music and for wasting official Municipal time on social sites, it is for this reason that the Municipality has come up with the following items guidelines for acceptable internet usage:

7. Accessing bank sites for online banking
8. Searching for information relevant to your line of work
9. Visit other Municipalities websites for best practises
10. Visit academic websites for personal development

3.6 Unacceptable uses of the Internet

The Municipality's Internet access may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or X-rated. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language is to be transmitted through the Municipality's e-mail or Internet system. Electronic media may also not be used for any other purpose which is illegal or against Municipal policy or contrary to the Municipality's best interest. Solicitation of non-Municipal business or any use of the Municipal e-mail or Internet for personal gain is prohibited.

Users must adhere to the following precautions when surfing the internet

1. Do not spend more than one hour a day on the internet
2. Do not enable automatic password saving
3. Avoid installing software from the internet without the ICT Unit authority
4. Do not enable pop-ups, active x and downloads of any other software.

5. Internet access shall be denied in respect of sites falling under the following categories:
    1. Abortion;
    2. Alcohol/Tobacco;
    3. Alternative spirituality/Occult;
    4. Arts/Entertainment;
    5. Auctions/Brokerage/Trading;
    6. Chat/Instant Messaging;
    7. For Kids;
    8. Gambling/ Pay to Surf;
    9. Games;
    10. Hacking;
    11. Humour/Jokes;
    12. Illegal Drugs;
    13. Intimate Apparel/Swimsuit;
    14. Personals/Dating, Sexuality/Alternative Lifestyles and Pornography;
    15. Phishing;
    16. Proxy Avoidance;
    17. Restaurants/Dining/Food and Shopping;
    18. Spyware Effects/Privacy concerns/ Spyware/Malware Sources;
    19. Open Image/Media Searches/Streaming Media/MP3s; and
    20. Violence/Hate/Racism/Weapons

3.7 Posting of Information to information Groups

User are discouraged from using Municipal internet to participate in discussion groups however should you find the need to participate in such groups it must be for work official business only in that case this policy shall apply.

3.8 Downloading of Software

Files downloaded from the internet can cause malicious damage to the Municipalities ICT infrastructure and create vulnerabilities within the network. Users are therefore not allowed to download files from any site other than the files downloaded from the site listed in 4.1.3 above.

3.9 Sending of Security Parameters

Sending security parameters over the internet can create serious security risks to the network and can result in loss of data. It is for this reason that users are prohibited from sending or saving passwords, log on details, bank account details and or any other information which may be used to hack the network.

3.10 International Transfer of Data

The internet connects users to networks worldwide across international boundaries and this allows users to transfer data between countries. User just note that transferring of data in the internet may be in breach to South Africa and other international laws. Users are therefore discouraged from transferring data across international boundaries. Should a need arise for the user to transfer data across international boundaries using Municipal infrastructure he/she must do so with prior authorisation from the Municipal Manager. Data must be encrypted as per clause 3.9 of this policy.

3.11 Setting up of Extra Services

The Municipality will provide its users with the minimum internet services required for them to do their work; users are prohibited from setting up any additional services without the prior approval from the IT division. Any requests for additional services must be requested for in terms of this policy.

3.12 User Anonymity

This policy prohibits users from participating in social sites, however should a user need to participate in user group forums for official Municipal business then they must do so by honest representation.

3.13 False Security Reports

ICT will request security reports from time to time on internet usage and users will be required to submit these reports. False security reporting will result in disciplinary action.

3.14 Establishment of Network Connections

Users will be provided internet access via a secure tunnel, Managers and other users will be granted access via wireless connection. Only network connections provided by the Municipality will be used on Municipal equipment.

3.15 Dial up Access

Dial up access will only be granted via a secure and encrypted network provided by the Municipality. Users are not allowed to setup dial up connection without prior authorisation from the ICT Unit.

3.16 Third Party Access

Third part connections can only be granted by the ICT Unit, users may not grant access to third parties.

3.17 Internet Monitoring and Filtering

The Municipality reserves the right to monitor, filter and restrict internet access at its own discretion. The Municipality also reserves the right to grant or deny internet access to users.

3.18 Non Compliance

Failure to comply with the provisions of this policy may result in the user's access rights being revoked by the ICT Unit.

SECTION FOUR

EMAIL USAGE

---

4. SECTION 4: email usage

4.1 Overview

Email and internet are similar in that they both run on the same on the same technology and both connect the users to the rest of the world at a click of a button. The Municipality has granted users access to the email for official use only. This policy has been developed to guide users on the usage of the Municipality's email facility. Every user is expected to adhere to this policy when using the Municipality's email services.

No users will be allowed to send e-mail that is defamatory, abusive, obscene, profane, fraudulent, harassing, embarrassing, indecent, intimidating, violent and in violation of copyright and RSA and international laws.

The policy covers the following domain in respect to Email usage:

1. Legal Risks
2. Legal Requirements
3. Best Practises
4. Personal Use
5. Confidentially Information
6. Disclaimer
7. System Monitoring
8. Email Accounts
9. Sending emails
10. Attachments to emails

The purpose of this policy is to ensure the proper use of Municipality's email system and make users aware of what the Municipality deems as acceptable and unacceptable use of its email system. The Municipality reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

4.2 Legal Risks

Email is a municipality communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email

seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of e-mail:

1. If you send emails with any rebellious, defamatory, offensive, racist or obscene remarks, you will be held liable.
2. If you forward emails with any rebellious, defamatory, offensive, racist or obscene remarks, you will be held liable.
3. If you unlawfully forward confidential information, you will be held liable.
4. If you unlawfully forward or copy messages without permission, you will be held liable for copyright infringement.
5. If you send an attachment that contains a virus, you will be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of e-mail. If any user disregards the rules set out in this Email Policy, the user will be fully liable and the Municipality will disassociate itself from the user as far as legally possible.

4.3 Legal Requirements

The following rules are required by law and are to be strictly adhered to:

- It is strictly prohibited to send or forward emails containing rebellious, defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify your supervisor.
- Do not forward a message without acquiring permission from the sender first.
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's email account.
- Do not copy a message or attachment belonging to another user without permission of the originator.
- Do not disguise or attempt to disguise your identity when sending mail.

4.4 Sending Emails

No users will be allowed to send e-mails with unverified information and/or unauthorized transactions to anyone.

The following, but not exhaustive, will constitute e-mail abuse which may result in instituting a disciplinary action against the user concerned:

11. Soliciting e-mails or Internet for commercial ventures, religious, political and personal causes or outside organizations;
12. Using e-mail for gossip, including personal information about users or others;
13. Emotive responses to municipality correspondence or work situations;
14. Forwarding e-mails likely to embarrass the sender or recipient;
15. Using the network for private ventures and/or personal gain; and
16. Any threatening or abusive e-mail received by users shall be brought to the attention of the executive manager who will take the appropriate action which may include legal action.

4.5 Attachments to E-Mails

17. Attachments shall be kept to a maximum of 6 Megs.
18. E-mail must be scanned for the following conditions and where they occur, the message must be blocked and quarantined:
19. Attachments that could hide malicious code (e.g. exe file, MPEG etc.);
20. Prohibited words (words that are racist, offensive or obscene); and
21. Key known phrases, like those commonly used in chain letters or hoax viruses.

4.6 Best Practices

Users shall delete their e-mails (Inbox, Sent Items, and Deleted Items) on a regular basis to free up space on the server.
The Municipality considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Therefore, the Municipality wishes users to adhere to the following guidelines:

4.6.1 Writing Emails:

1. Write well-structured emails and use short, descriptive subjects.
2. The Municipality's email style is informal. This means that sentences can be short and to the point. You can start your e-mail with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of Internet abbreviations and characters such as smiley's however, is not encouraged.
3. Signatures must include your name, job title and company name. A disclaimer must be added in the beginning of the email (see Disclaimer)
4. Use the spell checker before you send out an email.
5. Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.
6. Do not write emails in capitals.
7. Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.
8. If you forward mails, state clearly what action you expect the recipient to take.
9. Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).
10. Only mark emails as important if they really are important.

4.6.2 Replying To Emails:

1. Emails should be answered within at least 8 working hours, but users must endeavor to answer priority emails within 4 hours.
2. Priority emails are emails from Customers, Government Departments, Members of the Public and other Municipalities.
3. When a user is on leave or away from work he/she must setup an out of office automatic reply and setup a rule to forward all priority emails to the supervisor.

4.6.3 Newsgroups:

1. Users need to request permission from their supervisor before subscribing to a newsletter or news group.

4.6.4 Maintenance:

2. Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.

4.7 Personal Use

Although the Municipality's email system is meant for municipality use, it allows the reasonable use of email for personal use if certain guidelines are adhered to:

3. Personal use of email should not interfere with work.
4. Personal emails must also adhere to the guidelines in this policy.
5. Personal emails are kept in a separate folder, named 'Private'. The emails in this folder must be deleted weekly so as not to clog up the system.
6. The forwarding of chain letters, junk mail, jokes and executable is strictly forbidden.
7. On average, users are not allowed to send more than 2 personal emails a day.
8. Do not send mass mailings.
9. All messages distributed via the Municipality's email system, even personal emails, are the Municipality's property.

4.8 Confidential Information

Avoid sending confidential information by e-mail. If you do, you must secure the information by including it in a Microsoft Word or Excel file and protecting it with a password. Then provide the recipient with the password by means of other communication, for instance by telephone.

4.9 Disclaimer

The following disclaimer will be added to each outgoing email:

'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. Finally, the recipient should check this email and any attachments for the presence of viruses. The Municipality accepts no liability for any damage caused by any virus transmitted by this email.'

4.10 System Monitoring

You must have no expectation of privacy in anything you create, store, send or receive on the Municipality's computer system. Your emails will be monitored without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, the Municipality reserves the right to take disciplinary action, including termination and/or legal action.

4.11 Email accounts

All email accounts maintained on our email systems are property of Municipality. Passwords should not be given to other people and should be at least changed once a month.

4.12 Email archiving

Users shall save and/archive their emails (Inbox and Sent Items) on regular basis to free up space on the server.
The ICT Systems Officer/ICT personnel reserves the right to delete e-mails, if space becomes an issue, but users on leave/away shall be taken into consideration in this regard and the user in question shall first be informed before deletion takes place.

4.13 Monitoring of Emails

Private e-mail correspondence should be limited to a minimum, the quantum will be regulated.

Chain letters shall not be permitted.

E-mail sent by a user is the express property of the MLM but this excludes any email where a copyright applies.

The MLM has the right, but not the duty, to monitor all e-mails to ensure compliance with this policy.

The following disclaimer will automatically be added to all out going e-mails that will protect the MLM from any legal action as far as e-mail abuse is concerned:

"This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual/s or entities to whom it is/are addressed. If you are not the named addressee you should not disseminate, distribute copy or alter this e-mail.
Please delete it immediately.

Any views or opinions presented in the e-mail are solely those of the author and MIGHT not represent those of the Mhlontlo Local Municipality.

Although reasonable precautions have been taken to ensure that no viruses are present in this e-mail, the Mhlontlo Local Municipality cannot accept any responsibility for any loss or damage arising from the use of this e-mail or its attachments."

SECTION FIVE

NETWORK USAGE

---

5. SECTION 5: Network Usage

5.1 Overview

Users of the Municipality's network and computer resources have a responsibility to properly use and protect those information resources and to respect the rights of others. This policy provides guidelines for the appropriate use of information technologies.

The purpose of the Computer and Network Usage Policy is to help ensure an information infrastructure that supports the basic operations of the Municipality. Computers and networks are powerful enabling technologies for accessing and distributing the information and knowledge developed at the Municipality and elsewhere6. As such, they are strategic technologies for the current and future needs of the Municipality. Because these technologies leverage each individual's ability to access and copy information from remote sources, users must be mindful of the rights of others to their privacy, intellectual property and other rights. This Usage Policy codifies what is considered appropriate usage of computers and networks with respect to the rights of others.

Users of Municipality's information resources must respect copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other information resource users. This policy covers the appropriate use of all information resources including computers, networks, and the information contained therein.

Section headings are:

1. Policy Scope and Applicability
2. Policies
3. ICT Systems Officer Responsibilities
4. Information Security Officer Responsibilities
5. Consequences Of Misuse Of Computing Privileges
6. Cognizant Office
7. Related Policies

5.2 POLICY SCOPE AND APPLICABILITY

5.2.1 Applicability

This policy is applicable to all Municipal Employees, Councillors and to others granted use of the Municipality's information resources. This policy refers to all Municipal information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by the Municipality. This includes networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, servers, desktops, and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

5.2.2 Locally Defined and External Conditions of Use

The Municipality may define "conditions of use" for information resources under its control. The ICT Unit will be responsible for communicating this policy to all users.

5.2.3 Legal and municipal Process

The Municipality does not exist in isolation from the South African laws. Under some circumstances, as a result of investigations, subpoena or lawsuits, the Municipality may be required by law to provide electronic or other records or other information related to those records or relating to use of information resources ("Information records"). The Municipality may in its reasonable discretion review information records, e.g., for the proper functioning of the Municipality or for internal investigations.

5.3 POLICIES

5.3.1 Copyrights and Licenses

Computer users must respect copyrights and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected digital information.

5.3.2 Copying

Any material protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected material may not be copied into, from, or by any Municipal facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

5.3.3 Number of Simultaneous Users

The number and distribution of copies of copyrighted materials must be handled in such a way that the number of simultaneous users in the Municipality does not exceed the number of original copies purchased by the Municipality, unless otherwise stipulated in the purchase contract or as otherwise permitted by copyright law.

5.3.4 Copyrights

All copyrighted information (text, images, icons, programs, video, audio, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of digital information is subject to the same sanctions as apply to plagiarism in any other media.

5.3.5 Integrity of Information Resources

Computer users must respect the integrity of computer based information resources.

5.3.6 Modification or Removal of Equipment

Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others, without proper authorization from the ICT Unit.

5.3.7 Encroaching on Others' Access and Use

Computer users must not encroach on others' access and use of the Municipality's computers, networks, or other information resources, including digital information. This includes but is not limited to: attempting to access or modify personal, individual or any other Municipal information for which the user is not authorized; attempting to access or modify information systems or other information resources for which the individual is not authorized; sending chain-letters, unsolicited bulk electronic mail either locally or remotely; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known by

the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a Municipal computer, network or other information resource; or otherwise damaging or vandalizing Municipal computing facilities, equipment, software, computer files or other information resources.

5.3.8 Unauthorized or Destructive Programs

Computer users must not intentionally develop or use programs which disrupt other computer or network users or which access private or restricted information or portions of a system and/or damage software or hardware components of a system. Computer users must ensure that they do not use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users must not use network links for any use other than permitted in network guidelines. The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, including the Municipality, as well as criminal action.

5.3.9 Academic Pursuits

The Municipality recognizes the value of research on service delivery, computer security, and the investigation of best practises. The Municipality may restrict such activities in order to protect Municipality and individual computing environments, but in doing so will take account of legitimate pursuits.

5.3.10 Unauthorized Access

Computer users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access.

5.3.11 Abuse of Computing Privileges

Users of Municipality's information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the Municipality. For example, abuse of the networks to which the Municipality belongs or the computers at other sites connected to those networks will be treated as an abuse of Municipality's computing privileges.

5.4 Reporting Problems

Any defects discovered in system accounting or system security must be reported to the appropriate ICT Staff member so that steps can be taken to investigate and resolve the problem.

5.5 Password Protection

A computer user who has been authorized to use a password, or otherwise protected, account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the ICT Systems Officer.

5.6 Usage

Computer users must respect the rights of other computer users. Most Municipal systems provide mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of this policy and may violate applicable law. Authorized ICT Systems Officers may access computer users' files at any time for maintenance purposes. ICT Systems Officers will report suspected unlawful or improper activities to the proper authorities.

5.7 Prohibited Use

Use of the Municipality's computers, network or electronic communication facilities (such as electronic mail or instant messaging, or systems with similar functions) to send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or Municipal policy, such as under circumstances that might contribute to the creation of a hostile or work environment, is prohibited.

5.8 Mailing Lists

Users must respect the purpose and charters of computer mailing lists (including local or network news groups and bulletin-boards). The user of an electronic mailing list is responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the lists purpose. Persons sending to a mailing list any materials which are not consistent with the lists purpose will be viewed as having sent unsolicited material.

5.9 Advertisements

In general, the Municipality's electronic communication facilities should not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below).

5.10 Information Belonging to Others

Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords or other digital materials belonging to other users, without the specific permission of those other users.

5.11 Privacy

Users must always adhere to the provisions of this policy, access to information and Protection of Private Information Acts when dealing with private information.

5.12 Political, Personal and Commercial Use

5.12.1 Political Use

Municipal information resources must not be used for partisan political activities where prohibited by applicable laws, and may be used for other political activities only when in compliance with legislation, and other Municipal policies.

5.12.2 Personal Use

Municipality's information resources should not be used for personal activities not related to appropriate Municipal functions, except in a purely incidental manner.

5.12.3 Commercial Use

Municipality's information resources should not be used for commercial purposes, except in a purely incidental manner or except as permitted under other written policies of the Municipality or with the written approval the Municipal Manager. Any such commercial use should be properly related to Municipality's activities.

5.13 System Administrator's RESPONSIBILITIES

The Municipality shall appoint a systems administrator for each system and his/her responsibilities shall be as follows:

The ICT Systems Officer should use reasonable efforts:

1. To take precautions against theft of or damage to the system components.
2. To faithfully execute all hardware and software licensing agreements applicable to the system.
3. To treat information about, and information stored by, the systems users in an appropriate manner and to take precautions to protect the security of a system or network and the information contained therein.
4. To promulgate information about specific policies and procedures that govern access to and use of the system, and services provided to the users or explicitly not provided. This information should describe the data backup services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.

Where violations of this policy come to his or her attention, the ICT Systems Officer is authorized to take reasonable actions to implement and enforce the usage and service policies of the system and to provide for security of the system.

A system administrator/ICT Systems Officer may temporarily suspend access privileges if he or she believes it necessary or appropriate to maintain the integrity of the computer system or network.

5.14 Information Security Officer Responsibilities

The Municipality's' Information Security Officer or the person designated by the Municipal Manager shall be the primary contact for the interpretation, enforcement and monitoring of this policy and the resolution of problems

concerning it. Any issues concerning law shall be referred to the Legal Office for advice.

5.14.1 Policy Interpretation

The Information Security Officer shall be responsible for interpretation of this policy, resolution of problems and conflicts with local policies, and special situations.

5.14.2 Policy Enforcement

Where violations of this policy come to his or her attention, the Information Security Officer is authorized to work with the appropriate administrative units to obtain compliance with this policy.

5.14.3 Inspection and Monitoring

Only the Municipality's Information Security Officer or designate can authorize the inspection of private data or monitoring of messages (including electronic mail) when there is reasonable cause to suspect improper use of computer or network resources.

5.15 Consequences of Misuse of Computing Privileges

A user of the Municipality's information resources who is found to have purposely or recklessly violated any of these policies will be subject to disciplinary action up to and including dismissal, suspension, and/or legal action.

5.15.1 Cooperation Expected

Users, when requested, are expected to cooperate with ICT Systems Officers in any investigation of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.

5.15.2 Corrective Action

If the ICT Systems Officers have persuasive evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they should pursue one or more of the following steps, as appropriate to protect other users, networks and the computer system.

1. Provide notification of the investigation to Information Security Officer or designate, as well as the user's Manager, Head of Department or the Municipal Manager.
2. Temporarily suspend or restrict the user's computing privileges during the investigation.

A User may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the appropriate channels.

5.15.3 User Honour Code and Fundamental Standard

Unless specifically authorized by the Head of Department all of the following uses of a computer are examples of possible violations of the Honour Code:

1. Copying a computer file that contains another personal information or confidential information.
2. Copying a computer file that contains classified information.

SECTION SIX

FRONT END PERIPHERAL USAGE

---

6. SECTION 6: FRONT End Peripheral Usage

6.1 Overview

Front end peripherals shall be classified as any input, output and storage device which is used to access any Municipal information system or network. The list of peripherals shall be the following but is not limited to this list

1. Desktops
2. Laptops
3. Printers
4. Scanners
5. Screens
6. Memory sticks
7. Scanners
8. Telephones

The ICT Unit shall be responsible for designing the specifications for any front end peripheral and shall also configure; maintain and support the peripheral. The Security officer shall ensure that all peripherals are secured and users shall not temper; remove; installor open the peripherals.

The Municipality's assets unit will ensure that the peripherals are tagged and that they are inserted into the Municipality's fixed asset register.

The Municipality requires that all individuals utilizing Municipal Electronic Information Resources abide by the desktop and laptop security standards described by this policy.

6.2 Reason for the Policy

With the prevalent use of desktops and laptops in the Municipality, there is a risk that if computing system security vulnerabilities are left unsecured, then the information and data stored in personal computers are susceptible to theft and/or exploitation. This policy defines a number of safe computing standards to provide data protection on desktops and laptops.

6.3 Primary Guidance to Which This Policy Responds

This policy is established under the provisions of Municipality's Information Technology and Security Policy.

6.4 Responsibilities

The Security Officer is the responsible officer for this policy.

6.5 Policy Text

Computing technology is constantly evolving and new vulnerabilities are discovered every day; therefore, no system is completely immune to exploitation. Applying layered security controls will better protect Municipal computers from hackers.

The following steps must be adhered to by the User and/or the ICT Systems Officer/ Systems Administrator (SA) indicated in parenthesis following each of the items below.

1. Implement credible and reputable anti-virus software, perform continuous and/or scheduled scanning, and keep it up-to-date. An anti-virus program will protect your computer from malicious programs.

2. Implement anti-spyware to protect your private information. Spyware is a class of programs designed to steal personal information.

3. Enable the built-in firewall that is included in major operating systems and/or install a firewall application. A firewall is an application to restrict others from connecting to your computer

4. Regularly check for vendor security updates and apply them. Periodically, security weaknesses in the operating system and/or application are discovered and the vendor will then provide security updates to remediate such security exposures.

5. Establish strong password(s) syntax and protect your password(s). A password is used to provide authentication to an application and/or system.

6. If you are logged into a session, remember to log out after you are finished. Also, enable a password-protected screen saver when leaving your computer temporarily.

7. Keep your machine, especially laptops, physically secured.

8. Confidential and sensitive information must be safeguarded. Take appropriate measures (e.g., encryption for electronic information, physically secure physical media) to prevent unauthorized disclosure.

9. Scan all email attachments before opening them. Email is a method to spread malicious program via email attachments.

10. Refrain from using the save password feature applications because others who have access to your computer will also have access to your account.

11. Disable accounts which are not used and always change default passwords. Some operating systems come with predefined user accounts. These accounts are active by default.

12. Disable service which is not needed. Operating systems are packaged with services that are used by specific applications, such as ftp (for file transfer) or SMTP (for email).

13. Create regular backups of your data and files. Computers are like any machinery and can fail, and may result in the data and files that are corrupted or unrecoverable.

14. Be alert and aware of information stealing methods such as: social engineering, phishing scams, and shoulder surfing to obtain personal and sensitive information about you.

15. Sanitize your computer before donating or disposal.

16. Users are prohibited from saving data on the local hard drive unless the data is synchronised to the network drive daily.

17. Laptops and desktop and other front end peripherals are issued at the discretion of the Municipality.

6.6 Equipment on loan

18. User departments who hires new employees must make arrangement to have all necessary IT equipment that will be used by the new employee available during his/her first day at work.

19. No IT equipment must be loaned out for more than 3 months.

20. IT Unit must recall loaned equipment once 3 months' period has elapse.

SECTION SEVEN

PHYSICAL ACCESS AND ENVIRONMENTAL CONTROL

---

7. SECTION 7: PHYSICAL Access and Environmental Control

7.1 Overview

The main objective of this policy is to minimize disruption, damage, or loss of information and technology resources utilized by the Municipality and to comply with the Information Security Policy.

The Municipality must implement the requirements in this Policy to:

1. Limit physical access to information assets, information systems, and related equipment to authorized individuals;
2. Protect the facility and support infrastructure for information assets;
3. Protect information assets against natural disasters and environmental hazards; and
4. Provide the appropriate environmental controls and supporting utilities for information assets

The purpose of the Physical Access Control Policy (PACP) is to ensure the physical security of all information-holding assets owned by the Municipality, regardless of where (buildings, computers, files) or how they are stored (digitally, on paper).

The PACP aims to assist the Municipality to operate effectively and efficiently, to comply with legislation, information standards (ISO/IEC27001) and good practice, and to safeguard information-holding assets against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidentiality.

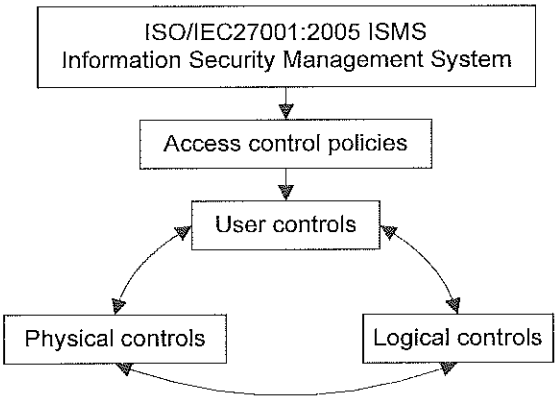
Rights of physical access are balanced by responsibilities, with all individuals granted access that is appropriate for their role / designated duties (including privileged access requirements i.e. secure rooms, cupboards).

The authority will have supporting policies (which may include legal or regulatory requirements) in place and will define procedures and provide mechanisms (for specific municipality areas) to ensure that access to

information-holding assets are handled within the appropriate laws and codes of practice.

All individuals must operate within this policy and procedural framework, and are accountable for their actions.

Understanding access control requires the understanding of the three access elements:



Physical – are actual objects that people can touch, see and use, manipulate or work with, e.g. a building, a computer or paperwork.

Logical – is non-physical (in the form of software or data), but is required and manipulated by the physical/user objects, e.g. a computer password, application programs, information stored in the computer such as a database

User - are the people that use and manipulate the two elements above.

7.2 Physical and Environmental Protection Control Selection

The selection of specific physical and environmental controls for the Municipality's information assets must be based on a risk assessment process. This assessment must include, at a minimum, the criticality of the information assets, defined risks to those assets, and the strengths and constraints of the facility containing the assets.

When the criticality of individual information assets or the number of co-located assets (such as in a data centres) increases, Municipality shall re-assess their physical security controls.

The Security Officer and the ICT Systems Officer will design and implement the environmental and access control specifications in terms of this policy.

7.3 Physical and Environmental Protection Procedures

The Security Officer will develop procedures to facilitate the implementation of the physical and environmental protection requirements as per this policy.

At a minimum, procedures must be implemented at the entity level and at additional levels as necessary (e.g., facility, information asset, information system)

7.4 Minimum Requirements for Physical Protection

The Municipality shall implement the following controls for facilities containing information assets, in accordance with the Municipality's assessment of risk:

I. Develop and keep current a list of personnel with authorized access to the facility (except for those areas officially designated as publically accessible), to include:

   a. Issuing appropriate access rights and related physical security credentials (e.g. identification cards, badges, keys, combinations, codes);
   b. Routinely review and approve the access list, rights, and credentials
   c. Have procedures for timely termination of physical access rights and recovery of physical security credentials for voluntary termination of employment and job transfers; and
   d. Promptly change physical access rights associated with an involuntary termination of employment and recover physical security credentials.

II. Restrict physical access to the facility to only authorized personnel by:
   a. Verifying individual access authorizations before granting access to the facility;
   b. Controlling entry to the facility using physical access devices (e.g. keys, locks, combinations, Card readers) and/or guards;
   c. Securing keys, combinations, and other physical access devices;
   d. Routinely inventorying physical access devices; and
   e. When physical access credentials are lost, stolen, or compromised physical security rights or corresponding devices must be promptly changed.

III. Control physical access to areas with critical or consolidated information assets (e.g. data centres, records storage areas):

a. Independently of the physical access controls for the facility; and

b. By limiting the number of personnel with physical access to the minimum necessary.

IV. Control physical access to information system distribution and transmission lines.

V. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

VI. Monitor physical access to the facility by:

a. Detecting and responding to physical security incidents;

b. Routinely reviewing physical access logs; and

c. Coordinating results of reviews and investigations with the entity's incident response capability.

I. Visitors must be authorized prior to accessing areas not publically accessible.

7.5 Minimum Requirements for Environmental Protection

A Municipality shall implement the following controls for facilities containing information assets, in accordance with the entity's assessment of risk:

a. Protect power equipment and power cabling from damage and destruction.
b. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of critical information systems in the event of a primary power source loss.
c. Employ and maintain fire detection and suppression devices/systems within the facility where the information assets reside, supported by an independent energy source.
d. Monitor and maintain within acceptable levels the temperature and humidity within the facility where information assets reside.

7.6 Responsibilities

7.6.1 User's responsibilities

1. Anyone who may access information-holding assets either directly or indirectly is responsible for following all appropriate procedures that relate to that asset

2. Users are responsible for their actions and should not take any action, which is outside the law or in breach of Municipal policies, procedures, guidelines or codes of conduct

3. Users are responsible for authorising access to information-holding assets under their area of control or responsibility

7.6.2 Manager's Responsibilities

4. To ensure that the controls deployed are proportionate to the sensitivity of the information-holding assets being accessed;

5. To implement and monitor this policy within their areas of responsibility and for ensuring that those for whom they are responsible, including visitors and contractors, are aware of and comply with the policy and associated guidelines;

6. To ensure that only authorised users are granted access to information-holding assets under their area of responsibility and for the adherence to relevant security policies by all users;

7. To ensure that all future building plans for both new buildings and renovations should take account of the need to install entry systems that will allow access, whilst maintaining security;

8. To ensure that all users are appropriately educated so that when accessing / using information-holding assets appropriate security measures are carried out;

9. To notify and seek guidance from the Corporate Information Security Officer or ICT Help Desk of all breaches of this policy;

10. To notify Human Resources (via normal procedures) of starters, movers and leavers to ensure the security / return of information-holding assets e.g. network access, keys etc;

11. To ensure that all users are taken through a formal "exit interview", by their line manager, when they end their employment with the authority. A checklist must be used to ensure any and all council property is returned, together with any access keys used during the employee's term of employment. A checklist template is available in the Municipalities data share point portal within thePipeline Assessment and Certification Program(PACP) guidelines and can be adapted for specific department requirements. This will also include a process to inform all relevant departments of the leaver's intent and to disable or remove, as appropriate, any access rights to council buildings and resources; and

12. To define the municipality requirements for business continuity management in association with the relevant staff in emergency planning and directorates.

7.7 Access to Council Premises

Access to council premises shall be restricted to ensure that only authorised users or visitors may gain entry. Sign in procedures for visitors at reception areas must be followed and where access is controlled via an electronic key entry system, the issue, configuration of access and disablement must be closely controlled in accordance with this policy.

7.8 EMERGENCY ACCESS ARRANGEMENTS

In the event of an emergency, users will need to contact their line management using the contact details contained in their department's Business Continuity Plan (BCP. If the event is outside normal business hours, DRP team will have instructions and contact details for the various directorates.

Depending upon the nature of an incident, the Emergency Planning Response Team could be called into action, taking control of the emergency. Senior management will need to coordinate the affected directorates and instruct staff accordingly and in line with their respective directorate's BCP for emergency access arrangements and where necessary and defined within their BCP, protection of sensitive information or assets.

7.9 Managing Network Access Controls

Access to the resources on the network shall be strictly controlled to prevent unauthorized access.

Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.

7.10 Controlling Access to Operating System Software

Access to operating system commands shall be restricted to those persons who are authorized to perform systems administration / management functions.

Access shall be operated under dual control requiring the specific approval of senior management.

7.11 Securing Against Unauthorized Physical Access

Physical access to the server room which shall be regarded as a high security area shall be controlled with strong identification and authentication techniques, at all times. Staff with authorization to enter such areas shall be provided with information on the potential security risks involved.

Physical access to the data centre, housing servers and supporting infrastructure shall be limited to the authorized personnel.

Access to the security area/s shall be justified, logged, and monitored.

7.12 Monitoring System Access and Use

Access shall be logged and monitored to identify and prevent potential misuse of systems or information.

7.13 Giving Access to Folder drives, Files and Documents

Access to folder drives, information and documents shall be carefully controlled, ensuring that only authorised personnel may have access to sensitive information.

7.14 Controlling Remote User Access

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques.

7.15 Accessing Municipal Network Remotely

Remote access to the Municipality's network and resources shall only be permitted provided that authorised users are authenticated, data is encrypted across the network, and privileges are restricted.

Authorised Users shall access the network through VPN.

7.16 Permitting Third Party Access

Third party access to the Municipal network/ICT systems shall only be permitted through a signed SLA

Third party access to the Municipal information/system may be permitted for the purpose of maintenance or operational support being or to be rendered by the third party concerned.

Third party access to the Municipal information shall only be permitted where the information and/or system in question has been, "ring fenced".

A register of authorised third party access users, as well as the access levels provided, must be reviewed regularly (at least quarterly for ongoing contracts and ad hoc when access is set up) by the ICT Unit to confirm that there is still a valid municipality requirement.

All third party logon accounts must be revoked when the arrangement terminates.

SECTION EIGHT

LOGICAL ACCESS CONTROL

---

8. SECTION 8: Logical access control

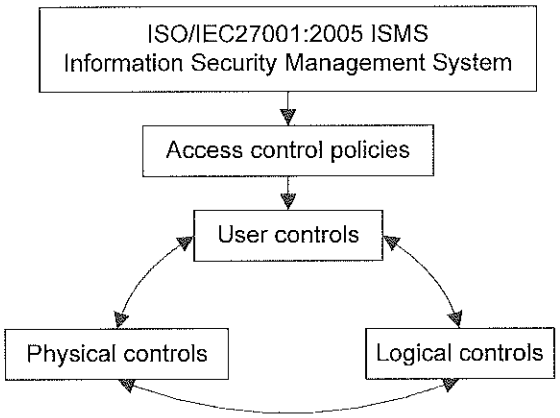
8.1 INTRODUCTION

The purpose of the Logical Access Control Policy (LACP) is to ensure the security of all information held in information systems owned by the Municipality, regardless of how they are stored (digitally, on paper or any other medium).

The LACP aims to assist the Municipality to operate effectively and efficiently, to comply with legislation, information standards (ISO27001) and good practice, and to safeguard information assets against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidentiality.

The authority will have supporting policies (which may include legal or regulatory requirements) in place and will define procedures and provide mechanisms (for specific municipality areas) to ensure that access to information-holding assets are handled within the appropriate laws and codes of practice. All users must operate within this policy and procedural framework, and are accountable for their actions.

Understanding access control requires the understanding of the three access elements:



8.2 Definition of terms

Physical – these are actual objects that people can touch, see and use, manipulate or work with, i.e. a building, a computer or paperwork

Logical – is non-physical (in the form of software or data), but is required and manipulated by the physical/user objects, i.e. a computer password, application programs, information stored in the computer such as a database

Users - are the people that use and manipulate the two elements above

Logical access controls provide a means of controlling what information users can view and manipulate, the applications they can run, and the modifications they can make. A set of LACP guidelines has been produced and highlights further details into counter-measures that support both technical and department requirements. Please refer to the LACP guidelines document for further guidance and information.

Logical access controls help protect the operating systems and other system software from unauthorised modification or manipulation (and thereby help ensure the system's integrity and availability).The integrity and availability of information by restricting the number of users and processes with access Confidential information from being disclosed to unauthorised Individuals.

8.3 POLICY STATEMENT

The Municipality shall implement measures to prevent unauthorised logical access, damage and interference to its information-holding assets, prevent loss, theft or compromise of its information assets and interruption of the council's activities.

The policy covers areas such as, but is not limited to (details of possible controls are given in the supporting guidelines document).

Only users authorized by their respective Heads of Department (Executive Manager) will be allowed access to the above-mentioned systems.

The Executive Manager will allocate and determine the level of access to each user.

All account creation requests shall be done in writing by the Executive Manager and forwarded to the ICT Systems Officer.

Access authentication, use of approved identification, passwords and two factor processes wherever necessary

13. Network access controls
14. Application access controls
15. Information access controls
16. Privileged use / user access controls
17. Encryption techniques
18. External access requirements e.g. VPN, 3rd party access etc.

8.4 RESPONSIBILITIES

8.4.1 User's responsibilities

19. Anyone who accesses any information-holding assets either directly or indirectly is responsible for following procedures for the information asset(s) they use or are responsible for.

20.

21. Users are responsible for their actions and should not take any action which is outside the law or in breach of council policies, guidelines or codes of conduct.

22.

23. Users should ensure that the controls deployed are appropriate for the use, circulation or distribution of the information for which they are responsible.

24.

25. Specifying and confirming that sufficient controls are in place to ensure the accuracy, authenticity and integrity of information.

26.

27. To ensure the confidentiality, integrity and availability of data they have created and/or modified (the person who created and manages information becomes the 'data owner')

28.

29. There are some special / privileged users who have extra responsibilities:

    1. Those users who are responsible for managing applications (application owners / custodians / administrators) on behalf of their departments, shall control access and usage of such applications and associated department information,

    2. ICT Systems Officers have the highest privileges permissible on all information-holding assets, be they physical or logical. For this reason, they must complete and sign a confidentiality agreement

8.4.2 Manager's responsibilities

30. To ensure that logical access controls are in place to protect their information-holding assets by determining access rights and carrying out risk assessments on the value and security of information assets, proportionate with the need to maintain the security of people, information and property.

31.

32. To implement and monitor this policy within their areas of responsibility and for ensuring that those for whom they are responsible, including visitors and contractors, are aware of and comply with the policy and associated guidelines.

33. To ensure that all users are appropriately educated so that when accessing / using information-holding assets and services appropriate security measures are carried out.

34.

35. To monitor the compliant use of their information; applications and systems.

36.

37. To report and seek guidance from the Information Security Officer or ICT Help Desk for all information security incidents.

38.

39. To notify Human Resources (via normal procedures), of movers and leavers to ensure the security / return of information-holding assets e.g. network access, return of keys and ID card etc.

40.

41. All employees shall be taken through a formal "exit interview" with their line manager, when they end their employment with the authority for whatever reasons. The checklist will be used to ensure that logical access controls will not be compromised when the user leaves or moves. A checklist template is available within the LACP guidelines and can be adapted for specific department requirements

8.5 Logical Access Control Policy Guidance

8.6 Access Controls	General access controls that should be considered
8.6.1.1 Type	8.6.1.2 Control details
Centralised access management	• Authorisation 42. Information classification 43. Management authorise access 44. Access request process
	Authentication – the following points should be considered 45. User IDs • Individual user IDs should be used • User IDs will not be shared unless senior management authorisation is approved • Access granted to users should be based on what the user needs to do their job and no more • Lock outs – screen savers should be implemented to automatically lock screens

8.6 Access Controls	General access controls that should be considered
8.6.1.1 Type	8.6.1.2 Control details
	• Limit duplicate log ins by the same user wherever feasible • Consider setting timed limits for access e.g. just allow access between office hours e.g. 07:00 till 19:00 (7.00 a.m. to 7.00 p.m.) • Consider disabling / removing out of the box user IDs and replacing them with bespoke ones Generic IDs • Should not be used unless there is a valid business reason to do so, which has been appropriately approved by senior management (AD level). • Where these are used, records/logs should be kept that would enable the use of generic IDs to be linked back to individuals i.e. who was using it when • Should, where possible, be limited such that only one person at a time is using it Passwords • Consider changing passwords on a regular basis • Consider the strength / complexity of passwords to be used e.g. admin accounts should use strong / complex passwords • Sharing of passwords is not permitted • Secure storage of admin passwords • Encrypted storage of passwords • When a password is initially granted / setup – the user should be required to change it when it is first used • Out of the box passwords should be changed 46. Biometrics • Fingerprint authentication • Secure USB encryption key • Secure encryption key-card • Facial • Voice • Third party access • Location based • Access control lists • Job / role based access - Access granted should be sufficient • for people to carry out their role, no more • Two factor authentication

8.6 Access Controls	General access controls that should be considered
8.6.1.1 Type	8.6.1.2 Control details
	• Folder and file permissions
	• Management and monitoring 47. Auditing / logging 48. Screen savers / automatic lock outs
Type of users	49. Privileged 50. Normal 51. Visitors 52. Partners 53. Suppliers 54. Contractors / temporary employees
Types of access	55. Network access • Use of Active Directory to authenticate users • Firewalls • Packet filtering • Restricted use of protocols • Detection and monitoring 56. Application access 57. Information access • Standard information (data) • Confidential / sensitive information (data) • Privileged use / user access • External access • Remote access • Firewalls • Port protection • Secure areas • Mobile devices • PDA / Smart phones • USB devices / drives / memory pens, etc. • CD, DVD and floppy disks etc.

8.6 Access Controls	General access controls that should be considered
8.6.1.1 Type	8.6.1.2 Control details
	• PCs and Servers • Loaned equipment

8.7 Use of hardware / equipment	Controls and issues around the use of hardware and equipment
8.7.1.1 Type	8.7.1.2 Details
Hardware / equipment controls	• Only approved hardware shall be used and installed by qualified ICT personnel
	• Restrictions on what hardware can be installed e.g. modems are not allowed unless there is a specific business reason to do so and, where applicable, not connected directly to the corporate network
	• Restrictions on who can change parameters / settings
	• Where feasible, restrictions to be applied on the usage of removable storage media (USB devices, etc.) • Where possible such devices should use encryption to protect data stored on them
	• Physical controls - See PACP and its guidelines
	• Access controls (see Access Control section)
	• Secure / restricted locations (see PACP)
Types of issues	58. Loss / theft 59. Unauthorised access **60.** Damage **61.** Malicious or fraudulent intent

8.8 Use of Software	Controls and issues around the use of software
8.8.1.1 Type	8.8.1.2 Details
Software controls	• Only Desktop & Infrastructure Services or department

8.8 Use of Software	Controls and issues around the use of software
8.8.1.1 Type	8.8.1.2 Details
	• management approved software should be installed by • qualified ICT personnel • Remove any unnecessary or unapproved software (software • that is not on the D&IS approved software list) especially • administration / programming software e.g. ftp programs, • magazine programs • Disable all unnecessary or unused services other than those • required for business needs/operations • Restricted access to file transfer type software - including • Reverse Address Resolution Process (RARP), Trivial File • Transfer Process (TFTP) • Permissions / privileged users e.g. only appropriate users • should be able to execute commands at system level • Firewalls (hardware and software) • Intruder Detection/Prevention Systems • Authentication (see access controls) • Logon controls (AD) – these should include: o Limit to one login account o Password protected screen savers o Day-time usage limits, e.g. 07:00 to 19:00 o Password controls o ID controls o RAS controls o Two factor authentication, etc. • Assess suitability of solution, consider the final location of Information that is to be stored, and e.g. is a web server the right place to store information - should it be on a restricted file system?
Types of issues	• Incompatibility with other approved software • Viruses and other malicious software • Impact on network performance and availability

8.8 Use of Software	Controls and issues around the use of software
8.8.1.1 Type	8.8.1.2 Details

	• Patching / Security updates
	• Inappropriate access
	  ○ Denial of service attacks
	  ○ Hacking, spoofing, etc.
	  ○ Eavesdropping
	  ○ SQL Injection
	• Misuse
	  ○ FTP
	  ○ Remote File sharing
	  ○ Deliberate acts
	  ○ Vandalism

Types of software	• Operating systems
	  ○ Microsoft Windows
	  ○ Unix / Linux
	• Applications
	• Email and Internet access

8.9 General Controls	**General controls that support the controls suggested in this document**
8.9.1.1 Type	8.9.1.2 Details
Confidentiality agreements	
• Policies	• Corporate Information and Security • Email and Internet policy • Logical • Physical • Acceptable Usage • Password

Data transmission	• Encryption
	  ○ Stored data
	  ○ Emails
	  ○ Portable media

Data Sharing	• See access controls • Links to DPA/FOIA and any other relevant acts or • regulations • Links to records management

SECTION NINE

VIRUS PROTECTION AND PATCH MANAGEMENT

---

9. SECTION 9: VIRUS PROTECTION AND PATCH MANAGEMENT

9.1 Overview

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event to computer software, data and/or the network. Viruses can be transmitted via email or instant messaging attachments, downloadable Internet files, USB disks, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to the Municipality in terms of lost data, lost staff productivity, and/or lost reputation.

This policy applies to all computers that are connected to the Municipality's network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both Municipal owned computers and personally-owned computers attached to the Municipal network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

9.2 Virus Protection

The ICT Unit to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by Users to help achieve effective virus detection and prevention.

9.2.1 Antivirus Policy Statement

a. The Municipality will provide an enterprise antivirus solution which will come with sufficient licenses for all user and devices attached to the network. The licenses will be renewed annually and to be renewed annually updates and patches shall be scheduled to run daily at night.

b. All computers attached to the Municipality's network must run standard and supported antivirus software. This antivirus software must be active all the time and must be configured to perform on-access real-time checks on all executed files and scheduled virus checks at present regular intervals. The virus definition files must be kept up to date all the time.

c. Any activity intended to create and/or distribute malicious programs onto the Municipal network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.

d. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she must report such incident to the ICT Unit immediately by e-mailing or by calling the Security Officer. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

e. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the ICT Unit.

f. Any virus-infected computer will be removed from the network until it is verified as virus-free.

9.2.2 Antivirus Software

The antivirus software package used must be installed on the main server, and migrated down to all Client computers thereafter.

9.2.3 Antivirus Software Installation

All Windows-based computers within the IT environment must have antivirus software installed with automatic updates enabled.

Desktop antivirus packages must be configured so that they cannot be disabled by the end user by configuring the requirement for a password to be entered to make modifications to the settings at the client.

The antivirus packages must be configured to scan all files on access and conduct a full scan on a weekly basis.

If a virus is identified, the software must be configured to provide an alert and clean the infected file or where this is not possible the file is quarantined.

9.2.4 Antivirus Software Updates

The antivirus packages must be configured to push updates automatically whenever a new version is released from a management console.

Testing of antivirus updates must only be conducted when there is a major engine change. This is to be tested in the test environment prior to being installed on the production environment.

The approval and release of antivirus updates are the responsibility of the IT department, who decide on the appropriate level of testing and manner of release of all hot-fixes and patches.

9.2.5 Antivirus Software Monitoring

Monitoring of all computers is the responsibility of the IT department. Since the process is automated; the main server must notify the IT department of any issues encountered or updates not installed, who then attended too it immediately.

9.2.6 Best Practices for Virus Prevention

1. Always run the standard antivirus software provided by the Municipality.
2. Never open files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
3. Never open files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.
4. Be suspicious of e-mail messages containing links to unknown Websites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
5. The Municipality's mail system scans all attachments for virus infections and blocks any trapped virus from being transmitted to client systems. The desktop antivirus on the client machine scans all email attachments for virus infections. Also, and by default the e-mail client, Microsoft Outlook, blocks attachments with critical file extensions.
6. Users should not alter the default email client configuration to override the security setup and send/receive banned extensions. A workaround to send/receive such municipality critical files is to compress the file using a file compression utility.
7. Never copy download, or install files from unknown, suspicious, or untrustworthy sources or removable media or untrustworthy sources or removable media.
8. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
9. Avoid direct disk sharing with read/write access. Always scan any removable media for viruses before using it.
10. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

11. Back up critical data and systems configurations on a regular basis and store backups in a safe place.
12. Regularly update virus protection on personally-owned home computers that are used for municipality purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

9.3 Patch Management

1. All security-related operating system and production software patches must be kept current and properly implemented.

2. Security patches must be deployed on a monthly basis or an exception basis for critical security patches.

3. Patches must be prioritised and tested by the ICT Unit before deployment.

4. Patch distribution must be scheduled so that there is little user intervention so that deployments can be done during off-peak hours.

9.3.1 Software and Firmware Updates Policy Statement

a. The Municipality will deploy an automatic software update services solution to manage and monitor critical software updates and patches to the applications, operating systems (both server and desktop) and firmware updates.

b. Users must always adhere to the ICT requests and guidelines in respect of software updates.

c. Users are not allowed to download and update any software without approval from the ICT Unit.

d. If a user receives a message on the Internet to update their software, they must consult the ICT Unit first before installing any software.

9.4 Responsibility of The ICT Unit:

1. ICT Unit is responsible for maintaining and updating this Virus Protection and Patch Management Policy. Copies of this policy will be posted on web site and the internal information portal. Check one of these locations regularly for updated information.
2. ICT Unit will keep the antivirus products it provides up-to-date in terms of both virus definitions and software version in use. The antivirus server shall be scheduled to check the for virus and software updates daily where possible hourly for the virus definition file and the software version.

3. ICT Unit will invest adequate efforts to identify clients who did not attempt to update their virus definitions file for more than 3 months and will take appropriate remedial actions.
4. ICT Unit will apply any updates to the services it provides that are required to defend against threats from viruses.
5. ICT will install antivirus software on all desktop workstations, laptops, and servers.
6. ICT will assist employees in installing antivirus software according to standards on personally-owned computers that will be used for municipality purposes.
7. ICT will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, CNS may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

9.5 responsibility of the USERS

1. Users must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.
2. Users Departments that allow employees to use personally-owned computers for municipality purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.
3. Users who don't employ staff with enough technical knowhow to ensure compliance with this policy should seek the assistance of ICT Unit to do so.
4. Users Departments' compliance with this policy shall be subject to audit.
5. All employees are responsible for taking reasonable measures to protect against virus infection.
6. Employees must not attempt to either alter or disable antivirus software installed on any computer attached to the Municipal network without the express consent of CNS and for a strictly limited period not to exceed in any case one working day.

SECTION TEN

ICT FAULT REPORTING AND MANAGEMENT

---

10. SECTION 10: ICT fault reporting and management

10.1 Overview

In this age of technology and information Municipalities and other organisations both private and public have become reliant on ICT to provide operational support so as to speed up delivery of services. The internet, email and other Information systems are critical to the Municipality as they allow for informed decision making.

To enjoy the maximum benefits of its ICT investment the Municipality needs to develop and implement a plan to detect and resolve incidents in time. This policy describes the procedure to control the ICT process of managing incidents at the Municipality. The process covers incident identification, analysis, resolution and review as conducted by the IT helpdesk.

10.2 Policy Statement

The Municipality will provide a helpdesk facility which will record, monitor and track all ICT related calls. All faults reported to the ICT help desk shall be handled in terms of this policy.

The purpose of this policy is to establish a uniform process for the incident management at the Municipality and to clearly define the fault escalation and priority process and procedures.

10.3 Incident Reporting

The ICT Unit shall ensure that there is a central number which users will call when reporting and incident, an email address will also be setup by the ICT Unit to enable users to log calls via email.

10.4 Incident Types

The ICT incidents shall be classified in as per the following high level categories: Security. Network, Server, Software, Application and User

10.5 Reporting an Incident

Any user requiring ICT assistance in resolving faults must log it with the designated ICT helpdesk. To log a call, the user will need to know the nature of the fault, their username and details of their equipment.

10.6 Logging of The Incident

The ICT Unit will ensure that there is a call logging and monitoring system in place, this system must have an automatic call escalation and alerting functionality.

10.7 Incident Priority

The server and any network device have the highest priority on the call list followed by application and finance system users. The priority will be set as follows

1. Sever,
2. Network Devices,
3. Critical application being: finance, payroll, GIS and other applications,
4. Internet and Email,
5. Senior Management,
6. Personal Assistants to the Managers and Committee Officers and
7. All other Users

10.8 Incident Assignment

The assignment of incidents will be based on the availability of technicians, any incident which required hardware replacement etc. shall be referred to the vendor.

10.9 Escalation

The escalation of the incidents shall depend on the nature and priority of that incident. Server and applications shall be escalated to the next level within 4 hours from logging. The ICT Unit shall have a maximum of 24 working hours to resolve an incident unless it cannot be resolved due to hardware replacement or availability of parts.

10.10 Incident Reviews

The ICT Unit shall assess the incidents weekly and compile a monthly report on the incident analyses to reduce the number of incidents logs and to identify training needs for the users.

Incidents shall also be used to identify and plan for the deployment of new technologies.

SECTION ELEVEN

ACQUISITION AND PROVISION OF INFORMATION TECHNOLOGY RESOURCES

---

11. SECTION 11: ACQUISITION AND PROVISION OF IT RESOURCES

11.1 Overview

Upon joining Mhlontlo Local Municipality, new staff will be provided with the resources required to enable them to carry out their duties and be able to function effectively in their environment.

The Executive Manager of the department that has engaged a new staff member shall determine the working needs of that incumbent as defined by the municipality's organogram, and access to information technology resources shall be granted on WRITTEN authorisation by the Manager responsible for ICT services.

All personnel making use of ANY of the Information Technology resources of the municipality shall be required to sign a copy of this policy before any access is granted.

11.2 Policy statement

The Municipality is committed to complying with applicable compliance laws, rules and standards. Management and all employees must conduct all municipality activities in accordance with the Municipality's compliance standards in a manner that:

1. Supports the achievement of the Municipality's business objectives and financial soundness.
2. Will result in a low risk of non-compliance with the letter and spirit of the compliance laws, rules and standards.
3. Ensures that instances of non-compliance which arise are promptly resolved in a manner which minimizes the adverse consequences thereof.

11.3 Purpose / Aim

This policy shall outline the manner in which IT resources will be allocated to employees of the municipality and outline the procedure that will be followed in obtaining such.

11.4 Scope

This policy shall outline the manner in which IT resources will be allocated to employees of the municipality and outline the procedure that will be followed in obtaining such. The policy also covers the acquisition of IT resources.

11.5 Application of The Policy

The policy for the allocation of IT resources shall be applicable to: -

1. Officials: All municipal employees deemed qualified to use the service.
2. Councillors: All members of the municipal council.

11.6 Acquisition of IT Resources

Except for minor purchases, hardware shall be purchased through a structured evaluation process which shall include the development of a detailed Request For Proposal (RFP)/specification document.

11.6.1 Planning of acquisition of IT Resources

ICT representatives must be involved in the planning stage of new IT acquisition process.

11.6.2 Purchasing and Controlling IT Consumables

IT Consumables must be purchased in accordance with the Municipality's Supply Chain Management Policy with usage monitored to discourage improper use.

No purchase of ICT resources can be made without the involvement of ICT Unit.

The ICT Systems Officer /ICT personnel shall verify and approve specifications for all-new electronic information equipment and software prior to purchase by each department.

11.6.3 Service Level Agreements (Contracts)

All Service Level Agreements for IT services must be centrally managed by ICT Unit.

Contracts must be must exist to formalise all key relationships with current IT service providers for IT hardware and software maintenance, networks, telephony, etc.

These contracts should include the following:

3. Minimum required service levels
4. Key performance indicators (KPIs)
5. Requirements for monthly performance reporting from service provider
6. Penalties for contact violation or non-performance

11.7 List of IT Resources

The following is a list of the IT resources that acquired and issued by the municipality:

1. A laptop computer
2. A desktop computer
3. Access to a shared network folder (i.e. x drive)
4. Access to a printer
5. Access to telephone services
6. Access to Municipal Application Systems
7. An email address
8. Internet Access
    - Internal
    - External (via a 4G modem)

11.8 Allocations of computers

A member being employed as Senior Managers, Middle Managers and Coordinators will be eligible to a LAPTOP by virtue of the requirement that management may be required to work longer hours as well as from "out of office" locations that will enable them to effectively function within their environment.

The following are the specifications for desktop computers:

Product ID	HP ProDesk 400 G5 (4CZ31EA)
Operating System Type	Windows 10 Pro 64-bit
Storage	500GB HDD 7200 SATA
Optical Drives	SATA SuperMulti LightScribe DVD Writer
Memory	4GB DDR3 Synch DRAM PC3
Graphics	Intel Graphics Media Accelerator X4500HD
Processor	Intel Core i5-8500
Communications	Realtek 8111DL GbE Ethernet Controller
Warranty	HP Next Day Onsite Response - 3 Year Next Day Onsite

Issuing and usage of a laptop shall be restricted to the business of the Municipality, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices.

The following are the specifications for laptops of Senior Managers and MM:

Product ID	HP Elitebook x360 1030 G3
Operating System Type	Windows 10 Pro 64-bit
Storage	256 GB M.2 PCIe SSD
Ports	2 x Thunderbolt (USB Type-C connector) 1 x USB 3.1 Gen 1 x headphone/microphone combo 1 x HDMI 1.4 1 x External Nano SIM slot for WWAN 1 x AC power
Memory	4 GB 2133Mhz DDR4
Display	13.3" FHD UWVA ultra slim with Corning® Gorilla® Glass touch screen (1920 x 1080)
Graphics	Integrated: Intel® HD Graphics 620
Warranty	3 Years Warranty
Processor	Intel i5-8250U (2.80GHz 6th Gen)
Communications	HP lt4132 LTE/HSPA+ 4G Mobile Broadband

The following are the specifications for a high spec laptop computer for Managers:

Product ID	HP Elitebook 830 G5 (3JX98EA)
Operating System Type	Windows 10 Pro 64-bit
Ports	1 x Thunderbolt™ (USB Type-C™ connector) 2 x USB 3.1 Gen 1 (1 charging) 1 x HDMI 1.4b 1 x RJ-45 1 x docking connector 1 x headphone/microphone combo
Storage	256 GB M.2 PCIe SSD
Memory	8 GB 2133Mhz DDR4
Display	13.3-inch Full HD UWVA Display (1920 x 1080)
Graphics	Integrated: Intel® HD Graphics 520
Warranty	3 Years Warranty
Processor	Intel Core i7-8550U
Communications	HP lt4132 LTE/HSPA+ 4G Mobile Broadband

The following are the specifications for a high spec laptop computer for Assistant Managers:

Product ID	HP Probook 640 G4 (3ZG54EA)
Operating System Type	Windows 10 Pro 64-bit
Storage	256 GB M.2 PCIe SSD
Memory	8 GB 2133Mhz DDR4
Ports	1 x USB 3.1 Type-C™ (charging) 3 x USB 3.1 Gen 1 (1 charging) 1 x HDMI 1.4 1 x RJ-45 1 x VGA 1 x headphone/microphone combo 1 x AC power 1 x docking connector
Display	14" diagonal HD SVA BrightView WLED-backlit (1366 x 768)
Graphics	Intel® HD Graphics 520
Warranty	3 Years Warranty

Processor	Intel Core i5-8250U
Communications	HP lt4132 LTE/HSPA+ 4G Mobile Broadband

The following are the specifications for a high spec laptop computer for Civil Technician:

Product ID	HP Probook 470 G5 (2VQ23EA)
Operating System Type	Windows 10 Pro 64-bit
Storage	1TB 5400rpm Hard drive
Memory	8 GB 2133Mhz DDR4
Ports	1 x USB 3.1 Type-C™ Gen 1 (Power Delivery, DisplayPort™) 2 x USB 3.0 1 x USB 2.0 (1 powered port) 1 x HDMI 1.4b 1 x VGA 1 x RJ-45 1 x AC power 1 x headphone/microphone combo jack
Display	17" 17.3 FHD LCD
Graphics	GeForce 930MX Dedicated DDR3 Graphics
Warranty	3 Years Warranty
Processor	Intel Core i7-8550U

The following are the specifications for a high spec laptop computer for municipal officials and finance interns:

Product ID	HP Probook 450 G5 (2RS09EA)
Operating System Type	Windows 10 Pro 64-bit
Storage	500GB 5400rpm Hard drive
Memory	4 GB DDR4 2400MHz
Ports	1 x USB 3.1 Type-C™ Gen 1 (Power Delivery, DisplayPort™) 2 x USB 3.0 1 x USB 2.0 (power port) 1 x HDMI 1.4b 1 x VGA 1 x RJ-45 1 x AC power 1 x headphone/microphone combo jack
Display	15.6" High Definition Anti-Glare LED
Warranty	3 Years Warranty

Processor	Intel Core i5-8250U

Persons who are issued with portable computers and who intend to travel for municipality purposes shall be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimize the risks.

Laptop computers are to be issued to, and used only by, authorised employees and only for the purpose for which they are issued for.

Line management shall authorize the issue of portable computers.

The information stored on the laptop shall be suitably protected at all times.

Off-site computer usage, whether at home or at other locations, may only be used with the authorization of line Management

Usage shall be restricted to municipality purposes, and users shall be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures.

All portable computing equipment shall be insured to cover travel domestically and/or abroad.

Any member of staff, whose responsibilities are such that their work requires that EXTENDED periods are spent outside their offices in the carrying out of their duties, may through their General Managers request that a mobile device be allocated to them. All other members will be granted access to a desktop computer so that they may function within their environment.

From time to time students and interns are engaged by the Municipality. These temporary staff members may be required to share computer resources. The department that has engaged the services of temporary staff shall provide the IT equipment required, depending on the availability of such resources within the environment where they may be placed.

11.9 Access to A Shared Network Drives

All users shall be granted access to a shared network folder/drive for purposed of storing work related information. The stored information shall be included in the municipality's daily backup procedures.

Storage of personal files (music, videos, pictures, etc) is prohibited. ICT reserves the right to remove such files from the server in the interest of saving disk space.

11.10 Access to A Printing Facility

All users shall be granted access to the network printers for purposes of document production. Users with special requirements for printing confidential and sensitive information shall be granted access to a localised printing facility (office printer).

The following are the specifications for printers:

- Office jet with a minimum of 4 Megs of RAM and print speed of 10 pages per minute.

Office printers may be considered and approved for individual users based on the nature of their job, by line management.

Network printers shall be centralised and be managed and/or controlled under the supervision of Corporate Services Department.

Information classified as Highly Confidential or Top Secret, may never be sent to a network printer without there being an authorised person to safeguard its confidentiality during and after printing.

The MLM reserves the right to change specifications from time to time in order to keep up with the latest technological developments.

11.11 Access to Telephone Services

All qualifying employees shall be granted access to the municipality's telephone services through the use of a Personal Identity Number (PIN). The telephone credit shall be granted in accordance with the Telephone Management Policy. Application forms are available at the ICT office.

11.12 Access to Application Systems

Only those employees that require Systems access in order to do their jobs may be granted access. The Departmental Manager under which responsibility for the System resides shall be required to append WRITTEN authority to any request for access to such System.

The following are systems that currently are in use, and the departments under which they currently reside.

APPLICATION SYSTEMS	RESPONSIBLE DEPARTMENT
Promun	Budget & Treasury

11.13 Email Access

All third parties requiring access to the municipality's email facility will be granted such on receipt by the Information Technology Office of a written request approved by the user Manager. Application forms are available at the ICT office.

11.14 Internet Access

All third parties requiring access to the municipality's internet facility will be granted such on receipt by the Information Technology Office of a written request approved by the user Manager. Application forms are available at the ICT office. External access to the internet shall be granted in accordance to the Internet policy.

11.15 Risk Issues & Handling of mobile equipment

Due to the mobile nature of laptops, it must be recognised that extraordinary risks are associated with these devices. These are:

1. Theft of the device
2. Loss of the device
3. Damage to the device due to poor handling
4. Unauthorised access to sensitive data due to this data being contained on a device that has left the premises of the municipality.

As a precaution, users are advised to secure mobile devices in this manner:

5. Ensure that mobile devices are stored in a locked place
6. Ensure that laptop bags are stored in the boot of your car and not on the passenger seats

7. Ensure that confidential and sensitive information is not stored on removable

It must be borne in mind that the cost of mobile devices is approximately double the cost of a desktop device, and as such the budget requirement for the supply of these devices to all members is prejudicial to the municipality, and must be limited to those that really require such devices in order to fulfil their duties.

11.16 Limitation and Responsibilities Of Users

Users shall use the network in the way that it is intended to and not wilfully cause any disruptions to the network infrastructure.

Users shall not be allowed to reveal any unauthorized personal information of any employee in the MLM to any other party via electronic form.

Users shall not be allowed to disclose any confidential work-related information to any other party.

Users shall not be allowed to use their access to the network for any illegal activity.

No user shall be allowed to attach any equipment to the network or computers without prior authorization by the Executive Manager in consultation with the ICT Systems Officer.

Users shall not be allowed to use any of the MLM's equipment for solicitation of funds, commercial or promotional use.

Users shall not be allowed to flood the network intentionally.

Users shall not be permitted to provide user accounts to any other person.

Users shall not be permitted to provide FTP (file transfer protocol) service to any of their files.

Users shall not be allowed to use the network system for network games, chat rooms, Internet Relay Chat (IRC) or Instant Message channels.

Electronic Vandalism is strictly prohibited. (Electronic Vandalism is defined as: "any malicious attempt to harm or destroy equipment or data, the network or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, knowing\conscious creation and transmission of computer viruses").

Copyright material must not be placed, copied or redistributed on the network without the author's or owner's explicit written permission.

Only legal software with its license can be installed on a user's computer.

Users shall comply with all software licenses and copyrights on their computers.

Each user shall sign an acknowledgement of hardware and software in his/her use.

The user shall not switch off the computer at the ON/OFF switch or at the wall plug as this can corrupt the Operating System.

Users shall use the "Shut Down" feature in Windows to properly shut down their computer.

Users shall leave their computers switched on at all times as far as possible; but:

1. The user must reboot their PC at least once a week during working hours.
2. All users shall be responsible for frequent updates (windows, antivirus, etc.).

Access for one user to another user's PC can only be authorized by the Executive Manager or the users' superior and must be done in consultation with the ICT Systems Officer.

Each user shall be responsible for using his/her common sense and real world ethics to take precautionary measures to avoid violation of the objectives of the Network Policy.

It shall be the duty of every person to whom a laptop computer is issued by the Municipality to familiarise him or herself with the terms and conditions of the insurance policy relating to such laptop computer. Should such laptop computer be lost or damaged and the insurer declines to compensate the Municipality for such loss or damage by reason of such person not having complied with such terms and conditions, then such person shall be liable to make good such loss or damage to the Municipality at his or her own expense.

The Municipality reserves the right to have unlimited access within any reasonable time to all ICT equipment allocated to any users to monitor and/or enforce compliance with this policy.

11.17 Exit Procedure

The following process is to be followed when notification is received from Human Resources of an employee leaving the municipality. On receipt of a document notifying IT of an employee's resignation/termination, the following must be complied with:

1. Removal of access rights/privileges
2. Internet,

Email,

3. Network Access (username & password)
4. VPN security codes
5. Surrendering of Data
6. Returning of all assets

SECTION TWELVE

BACKUP AND RESTORATION

---

12. Section 12: Backup and Restoration

12.1 Overview

The purpose of this policy is to document the Backup Plan that would be necessary to perform and maintain the backups and archive operations of the databases and applications used at the Municipality.

This backup and restoration plan is a high level document outlining the backup frequency, storage, labelling and testing of backups and backup media. Detailed information relating to backup and restoration procedures for applications administered by the Municipality have been documented in the Backup and Restore Procedure.

12.2 Policy statement

The Municipality is committed to complying with applicable compliance laws, rules and standards. Management and all employees must conduct all municipality activities in accordance with the Municipality's compliance standards in a manner that:

1. Supports the achievement of the Municipality's business objectives and financial soundness.
2. Will result in a low risk of non-compliance with the letter and spirit of the compliance laws, rules and standards.
3. Ensures that instances of non-compliance which arise are promptly resolved in a manner which minimizes the adverse consequences thereof.

12.3 Purpose / Aim

The purpose of this document is to ensure standards are set to ensure backups of the system are made that can be restored to a correct and consistent state

after it has been damaged. An effective backup strategy describes a backup cycle and includes answers to the following questions:

1. Which parts of the system need to be backed up?
2. What type of backup is suitable?
3. When should they be performed?

12.4 Scope

This plan is applicable to the backup of applications, databases, operating systems, user data stored on file servers and middleware related to the Municipality.

12.5 Backup frequency

Backup of all data and applications shall be done daily as per the following schedule:

Daily Backup	**Monday to Friday**	**Workstation documents on Cibecs and Promun database**
Fortnightly Backup	**Fortnightly Backup**	**User data and mapped drives**
Monthly Backup	**Last working day of every Month**	**Full backup**

12.6 Backup media

In order to ensure backup redundancy and quick recovery of data and databases backup shall be made to Disk – Based devices and then to backup media on a monthly and yearly bases.

Backup copies of the files and program necessary to effect a recovery in the event of a disaster on server platforms should periodically be performed to safeguard the Council's information and data.

12.7 Offsite storage

Backup media should not be kept at the same location as the originating computer. This ensures that a mishap on the server does not affect the backup media, as they should be used for the recovery process.

Backups should be stored in a fireproof environment or safe. If no such environment exists, the backup media tapes should be stored off-site.

12.8 Backup success/failure

The success or failure of backups should be checked daily, investigated and corrective action taken if failure occurred.

Backup reports are to be filed and kept for at least three months.

Backups are to be scheduled to run during non-peak hours as backup systems tend to have a negative effect on the speed of the network, hence off-peak hours are recommended.

No Backup storage will be used without manufacturer's warranty (i.e. Backup devices shall only be used for (3) three years an, additional (2) two years extended can apply.

If a backup fail twice in the same media, and the media is suspected, the media is to be replaced and destroyed immediately.

Where backup procedures are inadequate or lacking, data may be lost or, effectively, unavailable, thus compromising the Council's business processes and operations

12.9 Testing of backup

A self – Test backup software shall be used to ensure that a backup has been successful and a restoration option is available. A backup restoration plan shall be formulated by the ICT Unit:

1. Daily backup media should be restored at least twice a year for key financial system and payroll system which should include one full restoration.
2. Monthly backup should as a minimum be restored once a year for key financial system and payroll.

Any changes that are introduced to backup configuration should also result in an additional backup and restore tests and the backup restoration plan should be updated accordingly. Changes can result from the Incident Management Procedure or the System Development Life Cycle.

Evidence of restoration tests performed, test results and resulting remediation should be retained for record purposes.

Backup copies of the files and program necessary to effect a recovery in the event of a disaster on server platforms should periodically be performed to safeguard the Council's information and data.

12.10 Retention and disposal of media

The retention and disposal of media shall be as follows:

Backup Type	Retention
Daily Backup (Local VMS)	45 days
Daily Backup (Munsoft & VIP)	(All)Offsite DR centre

12.11 Disaster Recovery Planning

The Disaster Recovery plan should be developed in cooperation with business process owners/personnel and based on risk based approach and should clearly define the roles and responsibilities of the recovery team members

DRP must be approved and tested to ensure the municipality can recover from the disaster

SECTION THIRTHEEN

NETWORK SECURITY

---

13. SECTION 13: Network security

13.1 Overview

The Network Management & Procedure Policy defines a network infrastructure that provides secure, available, and reliable data for all end-users connected to the Municipalities Network. As the Municipality grows it will continue to integrate technology into all facets of its operations, managing that technology becomes increasingly important. The following sections provide guidelines for servers, desktops, and laptops connected to the Municipality's network.

13.2 Intended audience

This Policy is intended for Technology Coordinators, Network Administrators, Network Engineers, Strategic Sourcing vendors and all others who are responsible for the configuration, management, or support of the Municipality's network environment. It assumes that the reader has general knowledge about network technologies and is familiar with common computer terminology. Additionally, the reader should understand that these steps may vary based on the configuration of a particular system. It is assumed that the reader has enough knowledge to access and use the programs and tools discussed without explicit instruction.

13.3 Scope

This policy will assist the Municipality in securing its desktop, laptops, and server operating systems for each of its sites.

13.4 Installing New Hardware

All new hardware installations are to be planned formally and all users concerned shall be notified prior to the proposed installation date.

13.5 Installing and Maintaining Network Cabling

Network cabling shall be installed and maintained by qualified engineers to ensure the integrity of both the cabling and the wall mounted sockets.

Any unused network wall sockets should be sealed-off and their status formally noted.

13.6 Removable Storage (Diskettes, USB memory sticks and CDs)

Only personnel who are authorised to install or modify software shall use removable media to transfer data to / from the Municipality's network.

13.7 Contracting or Using Outsourced Processing

Persons responsible for commissioning outsourced computer processing shall ensure that the services used are from reputable companies that operate in accordance with quality standards which should include a suitable Service Level Agreement which meets the requirements of the municipality.

13.8 Moving Hardware from One Location to Another

Any movement of hardware between the Municipality's workstations shall be strictly controlled by authorised personnel, managing asset register/s (i.e. Municipal assets and/or ICT assets).

13.9 Recording and Reporting Hardware Faults

All information system hardware faults are to be reported promptly and such call shall be recorded in a hardware fault register.

13.10 Maintaining Hardware (On-site or Off-site Support)

All equipment owned, leased or licensed by the Municipality shall be supported by appropriate maintenance facilities by the service provider concerned.

13.11 LAN and wan guidelines

13.11.1 LAN requirements

1. Every device connecting to the Network shall be named in terms of the Naming standards created by the ICT Unit i.e. PC –Asset number e.g. LT - 242994.

2. All computer equipment (network and standalone) must be asset-tagged and registered in the Municipality's asset register.

3. IP addresses must be automatically assigned to all desktops and laptops by the Municipality's authorised DHCP server, only servers and network devices shall be issued with static IP addresses.

4. The centralized anti- virus solution is the only anti- virus software allowed on the network.

5. All new purchases must be from pre-qualified vendors and named equipment approved by the ICT Unit in order to maintain uniformity and standards which will make it easy to manage patches and firmware updates.

13.11.2 Workstation Requirements

1. All computers attached to the network must at least have a 2.4 GHz genuine Intel processor or higher and must have a minimum 2GB of RAM with a 160 GB hard drive or higher.

2. Logging on to a domain is required for full service support and asset management and control.

3. All Administrative computers must be completely compatible with the WAN, capable of running the Municipality's administrative footprint, and hardwired for security purposes.

13.11.3 Server Requirements

1. All servers attached to the network must be approved by the ICT Unit.
2. Power PCs or equivalent must also be approved by the ICT Unit
3. All new servers need to be registered compatible with the Municipality's Network infrastructure and must adhere to the server standards.

13.11.4 Anti-virus Software

It is imperative to install anti-virus software and to keep the most current virus signatures on all Internet and intranet systems. The Municipality has to establish an enterprise anti- virus solution that automatically updates systems on all the Municipality's computers. The products used are approved by the ICT Unit and may only be installed and or uninstalled by the ICT Unit.

The Antivirus will automatically scan and detect viruses on the network and delete them, users are responsible for ensuring that they scan all memory disk etc. to ensure that they are not infected by viruses.

13.11.5 Desktop Management

Desktops will be managed using the windows domain controller; automatic updates will be controlled using Windows System Update Service (WSUS). Furthermore, local domains will need to establish a trust relationship with the enterprise domain.

13.11.6 Virtual Private Network

A VPN is a private network that uses a public network like the Internet to connect remote sites or users together. A VPN uses "virtual" connections to simulate real-world connections. The VPN provides connections to administrative services from workstations that are not connected to the administrative VLAN.

VPN client is intended to be used on an as-needed basis to access internal resources such as Mapper. The VPN permits secure, encrypted connections between the Municipality's private administrative network and remote users, and it insures that outside attackers cannot gain access through a connected client machine.

VPN benefits include:

1. Allowance of administrative access on instructional VLAN
2. Extended geographic connectivity
3. Improved productivity
4. Improved security
5. Provision of global networking opportunities
6. Provision of broadband networking compatibility

13.11.7 Standard USER APPLICATIONS SOFTWARE

Desktop or laptop allocated to users shall be allocated with the following minimum applications:

7. Microsoft Office 2013 or higher
8. Anti-virus software
9. Windows 7 Professional or higher

The MLM reserves the right to change specifications from time to time in order to keep up with the latest technological developments.

After new software and hardware purchases, the system administrator shall install helpdesk availability and IP address allocation.

All software and hardware purchases shall comply with the procurement policy of the MLM.

13.11.8 Content Filtering

ICT is responsible for providing content filtering for all users of the Municipality's network; as such, users may not have their own filtering systems. This includes all filtering software and/or hardware solutions.

13.11.9 Firewalls

ICT Unit must enable the built-in firewall that is included in major operating systems and/or install a firewall application. A firewall is an application to restrict others from connecting to your computer.

The ICT Unit provides the firewalls for all users. Users may not institute their own firewalls as they will disrupt communications, support, and network management.

The Municipality used a firewall device to manage and control VPN access and where necessary a VLAN is used.

13.11.10 New Servers

In order to add a new server to the network, ICT should configure the server and then complete and forward a Server Request Form to the Chief Information Technology Officer (GM-Corporate Services) for approval.

All servers must be configured with static IP addresses according to the Municipality's IP addressing guidelines. IP addresses can be viewed on the network diagram. If a server will be used throughout the Municipality, it is recommended that it be placed in the Main Server room so it is secure and centrally located within the LAN.

13.11.11 Restrictions

Users may not run:

1. Proxy servers, as it would conflict with required centralized content filtering
2. Remote Access Servers (RAS) for security reasons
3. WINS, which would conflict with services provided by the Domain Controller
4. DNS as it would conflict with services provided by the Domain controllers
5. DHCP, as it would conflict with services provided by the authorised DHCP server
6. Active Directory Services on any newly installed server without the approval of the ICT Unit

13.12 Server Installation and Configuration

13.12.1 Purpose

The following guidelines explain the process by which Windows-based servers are to be setup on the Municipalities network. These steps ensure that the devices meet the requirements for connection to the WAN.

13.12.2 Installation

Minimum configurations on server shall be provided by the ICT Unit and ICT shall ensure that these configurations are updated quarterly.

13.12.2.1 Pre-Windows Setup

i. Windows 2008 or higher is the standard Municipality's Windows OS, unless an application specifically requires otherwise.
ii. Make sure hardware is updated with the latest BIOS and firmware revisions.
iii. Make sure all RAID and SCSI drivers are obtained and loaded automatically during the initial Windows setup screens. If not detected by the setup disks, press F6 before setup runs.
iv. General RAID Guidelines:

a. **RAID0**: I/O intensive functions
b. **RAID1**: Lots of disk space; fault tolerance (mirror)
c. **RAID5**: Lots of physical disks and local data storage/retrieval

v. Delete all existing partitions, unless a vendor system utility partition exists.
vi. Partition Recommendations:
   a. ***C :\> 80GB,D:>70% of balance E :\> Balance of available hard drive space***
   b. ***Partitions must be configured to dynamic for extendibility***
vii. Format all partitions to be NTFS.
viii. Name and registration should be: ***Municipality's Name***
ix. Server licensing should be **per server**, unless otherwise specified.

13.12.2.2 Add-On/Removal during Install

i. Remove all default selections, e.g., Index Services, Accessories, etc.
ii. For remote accessibility, install Terminal Services.

13.12.2.3 Security Updates and Patches

i. Install the latest OS Service Pack
ii. Install the latest OS critical updates.
iii. Install the necessary OS hotfixes.
iv. Install the latest tested and approved IE for servers.
v. Install the latest IE updates.
vi. For IIS, see *Section 3.6.1* for detailed instructions on updates, patches, checklists and lockdown tools.
vii. The approved server anti-virus utility software
viii. Rename the default Administrator account to the approved account name,
ix. Create a separate administrator account for those who need local administrator rights and are not
x. Domain/Network Administrators review the *Windows 2012 Baseline Security Checklist* for any additional setup steps needed. The most
xi. current checklist is available on Microsoft's TechNet site A step-by-step guide for configuring enterprise security policies using the *MS Security Configuration Tool Set* is located on the Microsoft TechNet site.

13.12.3 Server Configuration

13.12.3.1 Computer Properties

i. Change display time to 0 seconds.
ii. If the server crashes, set to automatically reboot.
iii. Optimize performance for background services, if server's role is to run background network services such as IIS.
iv. Optimize performance for applications if server's role is to host heavily used applications.
v. Optimize performance for file sharing.
vi. Partition volume names should be: **C=System, D=Data, E=backup**.
vii. Page File should be set to:
C:\ =default minimum; set min and max to the same; ignore windows warnings.

D:\=1.5-2x Physical memory; set min and max to the same.

13.12.3.2 Network Properties

i. Identify designation network segment and configure appropriate TCP/IP network properties.
ii. Server optimization (file and print sharing properties):
    a. Maximize data throughput for file-sharing (user data, file storage).
    b. Maximize data throughput for network applications (client/server sharing applications).
iii. Make sure NICs are running at 100Mbps/Full Duplex.
iv. If only using one NIC, uninstall any teaming functions.
v. Uninstall any unnecessary network protocols and components, e.g., NetBEUI.

13.12.3.3 Miscellaneous

i. Set Display Properties to:
   a. 256 or 16-bit Colour

   b. No themes or screensavers

i. "My Computer" text = COMPUTERNAME (Machine Serial Number)
ii. "Network Places" text = Municipality Name Network
iii. Description = Users Surname and Name

13.12.4 Windows 2012 Server Configuration

This section outlines the steps necessary to secure computers running Windows 2012 Server either on their own or as part of a Windows NT or Windows 2000 domain. These steps apply to Windows 2008 Server and Windows 2012 R2 Servers.

13.12.4.1 File System

NTFS partitions offer access controls and protections that are not available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your server are formatted using NTFS. If necessary, use the CONVERT.exe utility to non-destructively convert your FAT partitions to NTFS.

Warning: If the CONVERT.exe utility is being used, it will set the security permissions (ACLs) for the converted drive to **"Everyone: Full Control**." Use the FIXACLS.exe utility from the Windows 2000 Server Resource Kit to reset the security permissions to values that are more appropriate.

Remove all unnecessary file shares

All unnecessary file shares on the system should be removed to prevent possible information disclosure and to prevent malicious users from using the shares as an entry to the local system.

13.12.5 Accounts

13.12.5.1 Administrator Account Password

Windows 2008 allows passwords of up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and non-printing ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or non-printing ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronized across multiple servers. Different passwords should be used on each server to raise the level of security in the workgroup or domain.

13.12.5.2 Disable or Delete Unnecessary Accounts

The list of active accounts for both users and applications on the system in the Computer Management snap-in should be reviewed regularly. Any non-active accounts should be disabled and accounts that are no longer required should be deleted.

13.12.5.3 Disable Guest Account

By default, the Guest account is disabled on systems running Windows 2012 Server. If the Guest account is enabled, disable it.

13.12.5.1 Accounts Configurations standards

To make it more difficult to attack the user account, follow the steps below for the user account configuration must be enabled:

1. Account lockout duration must be 15 minutes
2. Account lockout threshold must be 3 invalid logon attempts
3. Reset account lockout counter after 15 minutes
4. Enforcement password history remembers 24 passwords
5. Maximum password age must be 2 months

6. Minimum password age must be 1 day
7. Minimum password length must be 7 characters
8. Password must complexity requirements must be Enabled
9. Store passwords using reversible encryption must be Disabled

13.12.5.2 Administrator Account Configurations

Because the Administrator account is built- in to every copy of Windows 2008, it presents a well-known objective for attackers. To make it more difficult to attack the Administrator account, follow the steps below for the domain Administrator account and the local Administrator account on each server:

i. Rename the account to a non-obvious name, e.g., not "admin," "root," etc.
ii. Create a new Administrator account.
iii. Disable the local computer's Administrator account.
iv. Establish a decoy account named "Administrator" with no privileges. Scan the event log regularly looking for attempts to use this account.
v. Enable account lockout on the real Administrator accounts by using the local group policy utility.

13.12.6 Access Control List

13.12.6.1 Directory and File Protection

File and folder protection must be enables on all windows servers, use self-permission method to allocate access right to a user's folder.

13.12.6.2 Set Appropriate ACLs on all Necessary File Shares

By default, all users have Full Control permissions on newly created file shares. All shares that are required on the system should have permissions modified such that users have the appropriate share- level access, e.g., everyone = Read

Note: The NTFS file system must be used to set ACLs on individual files in addition to share- level permissions.

13.13 Security

13.13.1 Disable Unnecessary Services

After installing a Windows 2000 Server, any network services not required for the server role should be disabled. In particular, consider whether the server needs any IIS components and whether it should be running the server service for file and print sharing.

Disable the following unnecessary services:

1. IPSEC
2. DNS
3. DHCP
4. SNMP
5. Indexing Services

Avoid installing applications on the server unless they are necessary to the server's function. For example, do not install e-mail clients, office productivity tools, or utilities that are not strictly required for the server to do its job.

13.13.2 Protect the Registry from Anonymous Access

Windows Resource Protection (WRP) prevents the replacement of essential system files, folders, and registry keys that are installed as part of the operating system. It became available starting with Windows Server 2008 and Windows Vista. Applications should not overwrite these resources because they are used by the system and other applications. Protecting these resources prevents application and operating system failures. WRP is the new name for Windows File Protection (WFP). WRP protects registry keys and folders as well as essential system files. Ensure that WRP is enabled during run time and at installation.

13.13.3 Set Stronger Password Policies

To reinforce the system policies for password acceptance, use the Domain or Local Security Policy snap-in.

1. Set the minimum password length to at least six (8) characters.

2. Set a minimum password age appropriate to your network (typically between one (1) and seven (7) days).

3. Set a maximum password age appropriate to your network (typically no more than 40 days).

4. Set a password history maintenance (using the "Remember passwords" option) of at least four (4).

5. No three (3)-character sequences can be the same as the login name.

6. Three (3) of the following four (4) requirements must be met:

    a. Must contain an upper case letter (A – Z)

    b. Must contain a lower case letter (a – z)

    c. Must contain a numeric character (0 – 9)

    d. Must contain a special character (! #, ; : …)

13.13.4 Additional Security Settings

There is additional security features not covered in this document that should be used when securing servers running Windows 2012. Information about these security features such as Encrypting File System (EFS), Kerberos, IPSEC, PKI, and IE security is available on the Microsoft TechNet Security website.

13.13.5 Service Packs

13.13.5.1 Install the Latest Service Pack

Each Service Pack for Windows includes all security fixes from previous Service Packs. Microsoft recommends that you keep up-to-date on Service Pack releases and install the correct Service Pack for your servers as soon as your operational circumstances allow. The latest Service Pack for Windows applications and operating systems, is available on the Microsoft website. Service Packs are also available through Microsoft Product Support. More information is available on the Microsoft website.

Windows update services must be used to manage and deploy updates and services packs on the network through active directory. Users are not allowed to stop any updates. Updates must be downloaded daily at night from 20h00 and deployed to the users

13.13.5.2 Install the Appropriate Post-Service Pack Security Hotfixes

Microsoft issues security bulletins through its Security Notification Service. When a new security hot fix is announced, it should be immediately downloaded and installed on all servers. For information on automatic notification about hotfixes, visit the Microsoft website.

13.13.6 Verify Patches

The *Microsoft Baseline Security Analyser* (MBSA) is available via Microsoft's download site at http://download.microsoft.com. It is the appropriate utility to verify up-to-date Windows patches and should be run periodically after configuration changes or software updates, etc.

The analyser must be setup to run weekly using the scheduler.

13.13.7 Final System Check

1. Run MBSA/HFNETCHECK to verify up-to-date Windows patches.
2. Request for a thorough security check if.

3. Create a system Emergency Recovery Disk and label it with the machine name and date.

4. Synchronize clocks with the appropriate central timeserver as defined below.

NET TIME \\<*TIMESERVER*> /SET /YES

5. The following it will provide the Municipality's time servers.

13.13.8 Application-Specific Configurations

13.13.8.1 IIS

1. Install on data partition, i.e., D:\, E:\, etc.
2. If only using one IP address, make sure to unselect "**Use all assigned IP addresses**."
3. Select the assigned IP (do this for both WWW and FTP services options).
4. Install the default Web/FTP directories to the data partition (D:\inetpub).
5. Review the *IIS Baseline Security Checklist* for any additional steps needed (see Microsoft website)
6. Install the *IIS Cumulative Patch*
7. Install the *IIS Lockdown Tools*

13.13.8.2 Terminal Services (TS)

Under the Connections menu, select RDP Protocol Properties. If only using one IP address, be sure to unselect the default "**Use all network adapters**" option. Select the assigned IP.

13.13.8.3 SQL

1. Install to the data partition.
2. Install the latest Service Pack.
3. For security, assign an administrator account to the SQL Service instead of accepting the default.

13.13.9 Server Recommendations

13.13.9.1 Recommended Applications

The Municipality recommends specific software to extend server functionality as noted in the following chart:

1. Microsoft Windows Server
2. Microsoft desktop operating system
3. Microsoft Office

13.14 Naming Standards

13.14.1 Purpose

Deployment of enterprise e- mail, anti-virus software, and desktop management will require that all Windows users "login" to a central domain, or domain trusted by a central domain, and thus follow enterprise-wide naming standards.

This situation created potential name collisions between Sites and inherently limited the ability to provide centralized services. In addition, administration of a large environment also requires a naming convention that facilitates troubleshooting and account management. While a perfect naming convention does not exist, the recommended standards were developed to provide ease of use and unobtrusive renaming.

All computers and servers connected to the network must adhere to these naming standards. All local domains must follow a naming standard and must have a one-way in order to comply with proper security and maintenance.

The specific standards follow.

13.14.2 Workstation Naming Standard

Each workstation name is a 15-character fixed-length name composed of four fields, each serving a distinct purpose:

[Machine type initial] - [user initial] [user surname]

Lt-agqweta

13.14.3 Domain Naming Standard

The domain architecture will provide the Municipality with a foundation for initiatives that will facilitate greater reliability, expanded end-user services, and more cost-effective and efficient management. The architecture will be designed to accommodate our existing needs while providing scalability for future growth.

To prevent domain name collisions, all duplicate domains will need to be renamed according to the Domain Naming Standard. The Standard described below applies to all renaming situations as well as naming new domains.

Internal domain

[Mhlontlo][.] [gov]

E.g. Mhlontlo.gov

External domain

[Municipality][lm] [.] [Gov] [.] [Za]

e.g. Mhlontlolm.gov.za

13.14.4 USER NAMING standards

The naming resolution for the username shall me:

[First name] [Surname]

E.g. Asanda Gqweta = agqweta

13.14.5 email naming standards

The email address shall be the user's firstletternameandsurname@externaldomain of the municipality

e.g. agqweta@Mhlontlolm.gov.za

13.15 Security

The Windows operating system provides two main networking models for connecting computers. The first model is the workgroup model. This model is intended for connecting small groups of computers and users together. There is no shared security information and no centralized management. Each user must have an account on each computer to which they need access.

The second model is the domain model. A domain employs centralized security and policy administration. Users are usually issued accounts at the domain level and those accounts can be used to access various computers and resources in the domain. This domain model is the preferred method used by the Municipality to administer its

network environment. This model provides more control over users and security than the workgroup model, and it is the recommendation of the ICT Unit.

13.15.1 Purpose

Security is becoming more important as society relies more on information technology. It is important that assets be identified and classified both for security and for privacy considerations. The questions of availability and integrity must also be addressed.

Standards are created as guidelines to ensure that each unit is aware of its responsibility to the security of all other units. This ensures that the network environment will be secure from unauthorized external and internal attacks, and contingency plans can be put in place to minimize the impact of potential attacks to the total organization.

Due to customer-driven requirements, site-operating environments vary across the district; therefore, a cookie-cutter approach to security is not practical. Technology Coordinators, in conjunction with the ICT Unit, must weigh security with operational necessities. This section specifies the minimum requirements for securing a Windows operating system. The ICT Unit may implement additional security measures as necessary to optimize and ensure a secure environment overall. In addition to settings that may be specified through group policy or registry settings, there are several physical and operational requirements to a secure operating environment. This section details the necessary operational policies and physical security measures that should be in place.

13.15.2 System Installation

The following sections detail the steps that should be performed before, during, and directly after installation of servers, workstations, or laptops in order to ensure security.

13.15.3 Pre-Installation

Before connecting servers, workstations, or laptops to the Municipality's WAN, installers should ensure that all systems meet the minimum hardware requirements and that all systems are configured appropriately according to these guidelines.

For all new systems, vendors who supply custom software should also ensure that their software is compatible with Municipality's-approved images, i.e., pre- loaded software.

Virus protection is essential to maintaining a secure environment; therefore, the appropriate approved Anti-Virus should be installed and current at all times. ICT will provide licenses for the antivirus.

13.15.4 Installation

Installations should be tested for a reinstall prior to rollout. In addition, for a reinstall a full backup of the existing system is recommended before installation to safeguard against any potential problems.

13.15.5 Post-Installation

After installation, several actions must be performed. Many of these steps may be performed during the installation if a custom installation script is used, but the creation of such a script is beyond the scope of this document.

13.15.6 Account Requirements

Several new accounts are created as part of the default installation of windows desktop machines. As these accounts are well-known, they may represent prime attack targets. To help prevent attacks, the following accounts should be renamed or disabled: Help Assistant, Guest, Support_xxxxxxxx and Administrator.

1. *The Help Assistant, Guest, and Support_xxxxxxxx accounts should be disabled.*
2. *The **Administrator account** should be renamed to **root**.*
3. *The password of the root account must observe password complexity as follows: e.g. machineserialnumber#ADMIN@123*

The proper maintenance of user accounts is essential to the secure operating environment; therefore, all new accounts not utilized for more than 90 days should be disabled or deleted.

13.15.7 Recommendations for Local Computer Security

There are two necessary requirements for centralized services, such as desktop management and anti- virus protection: all devices must be visible and well-known to the network, and all must be in a domain. A by-product of this requirement is that all devices will be visible to each other in the Windows network places. Since this greatly simplifies the ability for someone to view machines at other Sites, it is important that proper security is configured on all devices to prevent inappropriate remote access to files. This section discusses known security deficiencies that are being addressed as the C.L.E.A.R. remediation project moves forward.

13.15.8 Network places

All computers and laptops will be joined to the domain using the naming resolution prescribed by the policy; therefore, they will all be visible on the network places with the username given prior to joining the domain.

13.15.9 Windows 9x File and Print Sharing

File and print sharing will be disabled on the local machine however it will be enabled on the file server, all access to files will be set to require authentication.

13.15.10 ICT Administrator Account

ICT will require higher access levels on the servers and on the machines so as to backup, install, uninstall and manage user accounts. The accounts will be setup as follows:

ICT group	Access	Group members
Helpdesk	Account management	Remote desktop into PDC and account manager.
Desktop Technician	Account Management and administrator	Administrator, account manager and remote desktop
Super Administrator	Enterprise admin	Enterprise Admin, Exchange Admin, domain admin, remote desktop.

13.15.10.1 Miscellaneous Security Settings

The following security settings will ensure optimal protection against unauthorized PC and/or network access.

13.15.10.2 Disable Remote Desktop Sharing

Remote desktop sharing enables several users to interact and control one desktop. This could allow unauthorized users to control the system; therefore, remote desktop sharing should be disabled.

13.15.10.3 Do Not Automatically Start Windows Messenger Initially

This setting prevents the automatic launch of Windows Messenger at user logon.

13.15.10.4 Wait for the Network at Computer Start-up &Logon

This setting determines if Windows waits for complete network initialization before allowing the user to logon. Part of this initialization is the application of Group Policy. If the setting is not enabled, then a user may logon before all Group Policy Objects (GPO) are obtained and processed, causing the user to temporarily operate under an incorrect security context. To prevent this from occurring, the setting should be enabled.

13.15.11 Recommendations for New Domains

Because every domain that is added to the infrastructure introduces increased overhead, complexity, and cost, it is important to fully understand the business drivers associated with the decision to introduce a new domain. This business driver can be obtained from the ICT Unit.

13.15.12 Account Management

Every new user will complete the approved service request form which can be obtained from the ICT Unit or from the human resources office. The user will complete the form and send it through relevant line Managers for approval. Once the form is approved it will be sent to ICT who will then create a username and password for the user and give the user relevant access to the approved resources.

ICT will keep a file for every user in a locked cabinet and shall ensure that all new users received induction into the network before they can sue it. If a user will be required to work with sensitive and confidential information, then ICT will ensure that the user is taken through the necessary security vetting process.

13.15.13 Domain Scenarios

Below are several trades-offs that must be considered when determining the best approach for implementing additional domains:

Account Management: A domain requires someone to add, create, and modify user accounts, passwords, profiles, security and other attributes. A major goal of the centralized domain is to automate the creation of user accounts in line with this policy. In some cases, Sites may want to perform account management to meet business needs regardless of the account management overhead.

Explicit Trusts: Each domain in another forest requires a manual trust be established with the INSTR domain. Trusts can break during WAN outages, requiring periodic

maintenance. As the number of trusts increases, the probability also increases that users and support staff will be impacted by a trust breaking.

Security: Managing a domain controller requires significant responsibility. Inadvertent schema changes or mass object creation on an enterprise domain can cause excessive replication traffic and can create a denial of service condition. In addition, a domain administrator has full access to all directory objects on a domain controller and can take ownership of objects in the configuration and schema using services on the domain controller. Therefore, domain administrators should be trusted individuals within Sites and the CPS environment. In general, the chance for security vulnerabilities to be discovered and exploited is increased as the number of domains increases.

DNS Configuration: Separate forests require special DNS settings in order to establish trusts properly with the INSTR domain. These settings can be problematic to manage and may depend on individualized workstation settings.

WAN Traffic: Implicit and explicit trusts require additional WAN traffic and therefore, latency, to authenticate users for inter-domain resource access. There is always a balance between user logon/authentication traffic and replication traffic.

Fault Tolerance: With no local DC, the WAN link is a single point of failure.

Additional Hardware Required: Active Directory represents a single point of failure and as such, a minimum of two DCs should be utilized maintaining a database. Alternatives such as restoring AD from tape can be problematic since all existing information such as user/group account changes, passwords, trusts, etc., can be lost from the time of the most recent backup. Workstations may require a technician visit to re-join them to the domain due to secure channel synchronization failure. In addition, it is not best practice to host web services from a DC due to the security risks present in most web applications.

13.16 Computer Imaging Requirements and Procedures

13.16.1 Purpose

This section details the Municipality's hardware and software requirements and procedures for installing multiple computers with a single image. It is intended for Strategic Sourcing vendors, Municipal Technology Coordinators and others involved in providing and supporting computer equipment to the sites.

13.16.2 Requirements

All new equipment purchased by the Municipality should be acquired from Strategic Sourcing vendors. *Ask the ICT Unit for the approved hardware needs.* The LAN management team requires the following from Strategic Sourcing partners and others who might image the computer equipment:

1. All hardware sold from a Strategic Sourcing vendor must be approved by the
2. All hardware sold must be asset-tagged per the asset tagging and tracking policy
3. Equipment must adhere to the terms and regulations of this policy.
4. Machines must come with a 3 years onsite next business day warranty

13.16.3 instructions

The ICT Unit will provide a list of instructions to be followed when imagine a machine and shall keep a register to track all images used by the Municipality

13.16.4 Installation Checklist

Before connecting servers, workstations, or laptops to CPS's WAN, installers should ensure that all systems meet the minimum hardware requirements and that all systems are configured appropriately according to this document.

For all new systems, vendors who supply custom software should also ensure that their software is compatible with the Municipality's-approved images, i.e., pre-loaded software.

Basic steps required for new systems include:

1. Connect to network
2. Rename PC – (see *Section 4: Naming Standards*)
3. Complete virus scan of machine
4. Configure antivirus to point to distribution server
5. Install critical updates from Microsoft – (see WindowsUpdate.com)
6. Install SMS client
7. Join network domain
8. Updating the anti-virus should occur automatically

13.16.5 Joining a Domain

The process of joining a domain from a workgroup will have two effects on the machines or above:

1. New user profile will be generated
2. Domain administrators' rights on local device will be enabled

The system will be joined into the MLM's domain.

Once the system has a domain account, a user will need to login with a domain account and password to use the workstation. Each Site has generic accounts, or users can login with their own domain accounts and passwords.

SECTION FOURTEEN

PROTECTION OF ICT EQUIPMENT (COMPUTER FACILITIES)

---

14. SECTION 16: Protection of IcT Equipment (COMPUTER FACILITIES)

14.1 Introduction

Environmental exposures are due primarily to naturally occurring events, such as lightning storms, earthquakes, volcanic eruptions, hurricanes and other types of extreme weather conditions. Hence, this Facilities Management (i.e. Server Room) Policy is to provide the municipality with principles to manage the protection of computer facilities and supporting environmental systems.

14.2Policy Statement

This policy provides the IT infrastructure and mechanisms to help the organisation realise its goals and objectives in setting IT environmental standards. Access to server rooms should be justified, authorised, logged and monitored. As such, this document applies to all personnel with access to server rooms, including those entering the premises, together with staff, temporary staff, clients, vendors, visitors or any other third party.

14.3 Purpose/Aim

The purpose of this policy is:

1. To outline the IT Environmental Standards.
2. To ensure access to key ICT facilities is restricted to individuals who are involved in the operation and maintenance of such facilities, and is recorded.

14.4 Key Objectives

The following key objectives are critical and applicable to the municipality which houses and manages data:

14.5 Access Control

1. Require an electronic access system.
2. If no electronic system is in place the server room must be under lock and key.
3. All fire exits must be kept locked and protected by a break glass system to ensure they are not used as a point of routine access or exit.
4. All windows must be adequately secured to prevent access.

14.6 Fire Control

1. Must have appropriate fire suppression systems in place which comply with all relevant health and safety legislation and have good access to appropriately signed fire exits.
2. Must have a fire detection system that automatically informs an appropriate person who reacts according to a defined process.

14.6.1 General

a. The approved contractor shall supply, install, commission and hand-over an approved fire protection system that complies with the requirements of SABS 0139 and SABS EN 54 and comprises an early-warning detection system as well as an automatic fire extinguishing system within the facility.
b. All equipment materials and design standards shall comply with the requirements of the Fire Protection Association (FPA) of South Africa, the Automatic Sprinkler Inspection Bureau (ASIB), the Fire Offices Committee (FOC) of the United Kingdom, the National Fire Protection Association (NFPA) of the USA, the DEAT of South Africa, the Montreal Protocol and the local fire authorities having jurisdiction.
c. Along with this, approved fire extinguishers compliant with the requirements of SABS 0105 shall be supplied and installed both inside and outside of each room making up the facility as well as plant rooms and/or DG canopies.
d. An integrity test to ensure that room is sealed must be performed.

14.6.2 Standard Requirements

The approved contractor shall provide, for each facility installation, the following:

i. A fire detection/protection system that conforms to the above requirements. Wherever possible, only Inergen, Argonite or pyroshield shall be utilised for the purpose of extinguishment.
ii. Detectors shall be strategically placed in room voids, floor voids and -where necessary – ceiling voids, in compliance with the design requirements of the stipulated standards.

14.7 Air Conditioning

An air conditioning system that operates 24 hours a day 7 days a week must be installed. It should be designed to keep the room to within the IT manufacturers' recommended specifications for temperature and humidity throughout the year.

14.7.1 General

a. Air conditioning equipment shall be supplied and installed by an approved contractor. It shall cater for the cooling requirements of the equipment to be housed in the facility as well as for any thermal loads generated by environmental equipment therein, by UPS systems therein, by lighting, by the introduction of fresh air, by solar radiation, by personnel and, by any other source that has an effect upon the determination of the air conditioning equipment selection.
b. Equipment shall, in General, have features that allow automatic restarting in the event of a power failure unless otherwise specified. Under these conditions

where multiple cooling circuits are employed, stepped or staggered re-starting of the cooling circuits shall be a mandatory requirement of this standard.

c. The equipment shall comply with the relevant requirements of SABS IEC 60335-2-40, SABS 0147 and SABS ISO 5151.

14.7.2 Standard Requirements

The approved contractor shall provide, as standard for each facility installation, the following:

i. Air conditioning equipment of a type appropriate for the application and conforming to the minimum requirements, of this standard as well as for equipment manufacturers' recommendations.

ii. Air conditioning equipment of a type that is readily available and locally supported in terms of spares holding, servicing, technical back up and that is warranted for at least one year from the date of installation.

14.8 Uninterruptible Power Supply (UPS)

14.8.1 General

a. The approved contractor shall supply, deliver, rig (where necessary) and install a UPS system that is dedicated to the supply of power to critical equipment within and essential to the facility and that can, under no circumstances, suffer momentary loss of power.

b. The battery backup associated with such UPS system shall be of sufficient duration to allow the local facility personnel to implement an orderly shutdown of equipment in the event of a failure of emergency power (from the standby diesel generator) to the UPS system itself.

c. Where facilities are unmanned it is a condition of this standard that remote networking via the UPS itself alerts facilities personnel of such a condition in order that an orderly shutdown of equipment can be implemented remotely.

14.8.2 Standard Requirements

The approved contractor shall provide, for each facility installation, the following:

i. An approved current technology UPS system of a type that is readily available and locally supported in terms of spares-holding, servicing, technical back-up and that is warranted for at least one year from the date of customer acceptance.

ii. The standby battery supplied with such a system shall be of a maintenance-free type that is warranted for a period of between 3 – 5 years from the date of customer acceptance.

14.9 Cleanliness

1. A periodic program of specialist cleaning must be in place. The frequency of cleaning must be appropriate to the environment and include under floor and above ceiling cleaning where there is a raised floor and false

ceiling. A member of the ICT Unit must be present when cleaning of the room is taking place.

2. Staff using the room may not eat or drink in the room and must keep the room clean and free of unnecessary contamination.

14.10 Policy Violation

3. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

15. User Declaration of indemnity

I _____ (Full Name and Surname) hereby declare that I am employed by Mhlontlo Local Municipality and by signing this policy I confirm that I have read and understand the content of this policy and further acknowledge that should I breach the policy the Municipality may take disciplinary action against me.

_____

_____

Signature Date

16. 18. Policy Approval

This Policy was approved at a full Council Meeting held on 31 day of May (Month) 2019 (Year) at MHLONTO Municipality.

Name and Surname	Designation	Signature
Nompumelelo Dyanti	Mayor	
[illegible]	MM	