INFORMATION & COMMUNICATION TECHNOLOGY USAGE AND SECURITY POLICY

Table of Contents

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 document 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:

- to inform users and managers of their responsibilities when utilising information assets, as well as for protecting technology and information assets
- to specify the mechanisms through which these requirements must be met
- to provide a baseline from which to acquire, configure and audit computer systems and networks in compliance with the policy
- to minimise disruption to and misuse of the Municipalities ICT infrastructure
- to ensure that the Municipalities resources are used for purposes appropriate to the business mission
- 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 Municipalities disciplinary code.

1.3 SCOPE

The policy applies to:

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

The policy deals with the following domains of security:

- Management of Information Security
- Management and Protection of ICT Infrastructure and Electronic communication

- Asset Management Physical Security and Environmental Controls
- System Acquisition development and maintenance
- Management of Human Resource Security and System Access
- Business Continuity Management
- Management of Third Party Relationships
- General S Usage and Controls of ICT Services
- ICT Risk Management

2 SECTION 2: 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:

- Business Continuity Plan - BCP
- Disaster Recovery Plan - DRP
- ICT Governance Framework
- Backup Procedures
- Network Diagrams
- SA Minimum Information Security Standards
- COMSEC Act 68 of 2002

2.1 POLICY APPROVAL AND AMENDMENT

Approval of this policy is vested with the Members of the Executive Committee of the Municipality. Advice and opinions on the policy will be given by:

- IT Steering Committee
- Internal Audit
- External Audit

Formulation and maintenance of the policy is the responsibility of the Municipality's ICT Division 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 Division will be the custodian of all strategic system platforms, communication systems and central computing facilities. The nominated system owners of each Directorate will be the custodians of the strategic applications under their control, while every user will be the custodians of the desktop systems and equipment under their control.

2.2 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 division will affect the necessary changes and the policy will be approved in terms of the Municipalities policy approval process.

2.3 APPLICABILITY

This policy applies to all councillors and officers 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.

2.4 ENFORCEMENT

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

2.5 TERMINOLOGY

Municipality shall mean UMNGENI Local Municipality.
ICT shall mean Information and Communication Technology.
User shall been anyone who connects to or used the UMNGENI ICT services.
Policy shall mean this policy.

SECTION THREE

INFORMATION SECURITY

3 SECTION 3: INFORMATION SYSTEMS SECURITY

The COMSEC 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 Municipalities 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:

- Information Security Responsibilities
- Classification of Information Sensitivity
- Access Control
- Management of Fixed Password
- Confidentiality
- Third Party Disclosure
- Acceptable Use of the Internet
- Encryption
- Electronic Mail
- Printing, copying and fax transmission
- Mobile computing and working from home
- Viruses, malicious software and change control
- Personal use of information systems
- Intellectual property rights
- System Development
- Reporting problems
- Non-compliance situations
- Disciplinary Measures

3.1 INFORMATION SECURITY RESPONSIBILITIES

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

3.1.1 INFORMATION OWNERS

The application and data owners responsibility shall be delegated to the head of that business unit and their responsibly shall be as follows;

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

3.1.2 CUSTODIANDS OF INFORMATION

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

- Ensure that Ensure that all appropriate personnel are aware of and comply with this policy.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

3.1.3 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.

3.1.3.1 INFORMATION SECURITY SECTION

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

3.1.4 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

3.1.5 EMPLOYEE RESPONSIBILITY

Ensure that all reasonable precautions are taken to protect business critical data against unauthorized access, especially data on notebooks 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-business critical data.

3.2 CLASSIFICATION OF INFORMATION SENSITYVITY

3.2.1 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.

3.2.2 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;

- Public
- Private
- Confidential
- Secret

- Top Secret

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

3.2.3 LABELLING

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

3.2.4 HANDLING INSTRUCTIONS

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

3.3 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.

3.3.1 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 shall be accessed during working hours.

3.3.2 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.

3.3.3 DEFAULT FACILITIES

The Municipal Facilities shall be classified as follows:

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

3.3.4 DEPARTURE FROM THE MUNICIPALITY

Any Visitor who has been granted 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.

3.3.5 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.

3.3.6 PREVILEGE 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.

3.3.7 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.

3.4 MANAGEMENT OF FIXED PASSWORD

3.4.1 CREATING PASSWORDS

The responsibility of creating passwords for all users in the Network is the 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.

3.4.2 CHANGING PASSWORDS

Users must change passwords after every 40 days. 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 division.

3.4.3 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.

3.5 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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;

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

3.10 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;

- Direct access via the VPN through Telkom line (Remote sites, MANCO, ICT)
- Remote Access via wireless, Dually authorised 3G card users
- Web Access(Any user with an email address and Active domain Account)
- 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.

3.11 VIRUSES, MALICIOUS SOFTWARE AND CHANGE CONTROLL

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 division 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 Division 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.

3.12 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 can it be used by anyone who is not employed or contracted to the Municipality.

Only the ICT division is allowed to test software on Municipal ICT infrastructure

3.13 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 division may make copies of any original software for backup purposes only.

3.14 SYSTEM DEVELOPMENT

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

3.15 REPORTING PROBLEMS

Incidents shall be managed in terms of this policy.

3.16 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.

SECTION FOUR

INTERNET USAGE

4 SECTION 4: INTERNET USAGE

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 business 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;

- Employee responsibilities
- Restrictions
- Non Restrictions
- Standard Internet/Email Practises
- Acceptable use of the Internet
- Unacceptable Use of the Internet
- Posting of Information to information Groups
- Downloading of Software
- Sending of Security Parameters
- International Transfer of Data
- Setting up of Extra Services
- User Anonymity
- False security reports
- Establishment of Network Connections
- Dial up Access
- Third Party Access

4.1 EMPLOYEE RESPONSIBILITY

The display of any kind of obscene image or document on any Municipalities 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 Division.

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 division.

4.2 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:

- Downloading of files e.g. MP3, MPEG, EXE, WAV & other malicious Software
- Access to social sites e.g. Face book, MySpace or any other chat sites
- Accessing Pornography Sites.
- Visiting webmail sites e.g. Gmail, Yahoo, webmail etc.
- Downloading pirated software to be installed on Municipal Computers.

- Accessing music sites

4.3 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.

Online Banking
Government websites
Medical Aid sites
Academic website
Municipal Web site
Municipality's intranet and internet webpage

4.4 ACCAPTABLE 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:

- Accessing bank sites for online banking
- Searching for information relevant to your line of work
- Visit other Municipalities websites for best practises
- Visit academic websites for personal development

4.5 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 council's e-mail or Internet system. Electronic media may also not be used for any other purpose which is illegal or against council policy or contrary to the council's best interest. Solicitation of non-council business or any use of the council e-mail or Internet for personal gain is prohibited.

Users must adhere to the following precautions when surfing the internet

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

4.6 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.

4.7 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.

4.8 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. The ICT division will enforce all users to access the internet via the proxy server and the Municipalities firewall users are therefore prohibited from changing any internet security settings.

4.9 INTERNATIONAL TRANSFER OF DATA

The internet connects users to networks worldwide across international boundaries and this allows users to transfer data between countries. User must 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.

4.10 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.

4.11 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.

4.12 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.

4.13 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.

4.14 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 division.

4.15 THIRD PARTY ACCESS

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

4.16 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.

4.17 NON COMPLIANCE

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

SECTION FIVE

EMAIL USAGE

5 SECTION 5: EMAIL USAGE

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.

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

- Legal Risks
- Legal Requirements
- Best Practises
- Personal Use
- Confidentially Information
- Disclaimer
- System Monitoring
- Email Accounts

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.

5.1 LEGAL RISKS

Email is a business 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:

- If you send emails with any libelous, defamatory, offensive, racist or obscene remarks, you will be held liable.
- If you forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you will be held liable.
- If you unlawfully forward confidential information, you will be held liable.

- If you unlawfully forward or copy messages without permission, you will be held liable for copyright infringement.
- 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.

5.2 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 libelous, 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.

5.3 BEST PRACTICES

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:

5.3.1 WRITING EMAILS:

- Write well-structured emails and use short, descriptive subjects.
- 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 smileys however, is not encouraged.
- Signatures must include your name, job title and company name. A disclaimer must be added in the beginning of the email (see Disclaimer)
- Use the spell checker before you send out an email.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.
- Do not write emails in capitals.
- 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.
- If you forward mails, state clearly what action you expect the recipient to take.
- 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).
- Only mark emails as important if they really are important.

5.3.2 REPLYING TO EMAILS:

- Emails should be answered within at least 8 working hours, but users must endeavor to answer priority emails within 4 hours.
- Priority emails are emails from Customers, Government Departments, Members of the Public and other Municipalities.
- 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.

5.3.3 NEWSGROUPS:

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

5.3.4 MAINTENANCE:

- 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.

5.4 PERSONAL USE

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

- Personal use of email should not interfere with work.
- Personal emails must also adhere to the guidelines in this policy.
- 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.
- The forwarding of chain letters, junk mail, jokes and executable is strictly forbidden.
- On average, users are not allowed to send more than 2 personal emails a day.
- Do not send mass mailings.
- All messages distributed via the Municipality's email system, even personal emails, are the Municipality's property.

5.5 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.

5.6 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.'

5.7 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.

5.8 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 changed once a month. Email accounts not used for 60 days will be deactivated and possibly deleted.

SECTION SIX

NETWORK USAGE

6 SECTION 6: NETWORK USAGE

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 elsewhere. 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:

- POLICY SCOPE AND APPLICABILITY
- POLICIES
- SYSTEM ADMINISTRATOR RESPONSIBILITIES
- INFORMATION SECURITY OFFICER RESPONSIBILITIES
- CONSEQUENCES OF MISUSE OF COMPUTING PRIVILEGES
- COGNIZANT OFFICE
- RELATED POLICIES

6.1 POLICY SCOPE AND APPLICABILITY

6.1.1 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.

6.1.2 LOCALLY DEFINED AND EXTERNAL CONDITIONS OF USE

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

6.1.3 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.

6.2 POLICIES

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.2.4 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.

6.2.5 INTEGRITY OF INFORMATION RESOURCES

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

6.2.6 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 Division.

6.2.7 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.

6.2.8 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.

6.2.9 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**.**

6.2.10 UNAUTHORIZED ACCESS

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

6.2.11 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.

6.3 REPORTING PROBLEMS

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

6.4 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 system administrator.

6.5 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 system administrators may access computer users' files at any time for maintenance purposes. System administrators will report suspected unlawful or improper activities to the proper authorities.

6.6 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.

6.7 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.

6.8 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). Some public bulletin boards have been designated for selling items by members of the Stanford community, and may be used appropriately, according to the stated purpose of the list(s).

6.9 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.

6.10 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.

6.11 POLITICAL, PERSONAL AND COMMERCIAL USE

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.

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.

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.

6.12 SYSTEM ADMINISTRATOR RESPONSIBILITIES

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

The system administrator should use reasonable efforts:

- To take precautions against theft of or damage to the system components.
- To faithfully execute all hardware and software licensing agreements applicable to the system.
- 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.
- 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 system administrator 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 may temporarily suspend access privileges if he or she believes it necessary or appropriate to maintain the integrity of the computer system or network.

6.13 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.

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.

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.

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.

6.14 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.

Cooperation Expected
Users, when requested, are expected to cooperate with system administrators 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.

Corrective Action
If the system administrators 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.

- 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.
- 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

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:

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

SECTION SEVEN

FRONT END PERIPHERAL USAGE

7 SECTION 7: FRONT END PERIPHERAL USAGE

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

- Desktops
- Laptops
- Printers
- Scanners
- Screens
- Memory sticks
- Scanners
- Telephones

The ICT division 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 secured and users shall not temper remove or install 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.

Reason for the Policy

With the prevalent use of desktops and laptops in the Municipality, there is the 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.

7.1 PRIMARY GUIDANCE TO WHICH THIS POLICY RESPONDS

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

7.2 RESPONSIBILITIES

The Security Officer is the responsible officer for this policy.

7.3 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 System Administrator (SA) indicated in parenthesis following each of the items below.

- 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. (User and SA)

- Implement anti-spyware to protect your private information. Spyware is a class of programs designed to steal personal information.(User and SA)

- 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. (SA)

- 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. (SA)

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

- 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. (User)

- Keep your machine, especially laptops, physically secured. (User and SA)

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

- Scan all email attachments before opening them. Email is a method to spread malicious program via email attachments. (User)

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

- 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. (SA)

- 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). (SA)

- 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. (User and SA)

- 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.(User)

- Sanitize your computer before donating or disposal. (User and SA)

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

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

SECTION EIGHT

PHYSICAL ACCESS AND ENVIRONMENTAL CONTROL

8 SECTION 8: PHYSICAL ACCESS AND ENVIRONMENTAL CONTROL

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:

- limit physical access to information assets, information systems, and related equipment to authorized individuals;
- protect the facility and support infrastructure for information assets;
- protect information assets against natural disasters and environmental hazards; and
- provide the appropriate environmental controls and supporting utilities for information assets

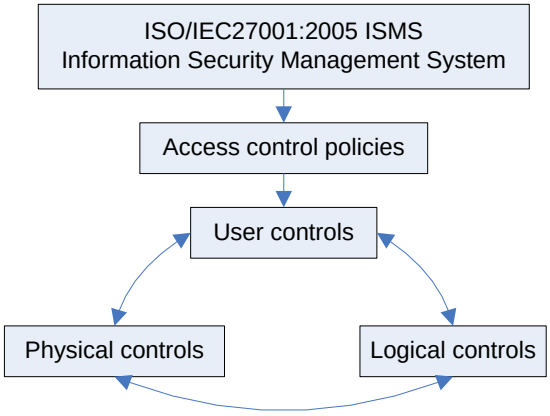
The purpose of the Physical Access Control Policy (PACP) is to ensure the physical security of all information-holding assets owned by the Municipality, regardless of where (buildings, computers, files) or how they are stored (digitally, on paper).

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 business 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.

8.1 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 Systems Administrator will design and implement the environmental and access control specifications in terms of this policy.

8.2 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)

8.3 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.

8.4 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.

8.5 RESPONSIBILITIES

8.5.1 USER'S RESPONSIBILITIES

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

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

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

8.5.2 MANAGER'S RESPONSIBILITIES

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

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

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

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

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

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

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.

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 the PACP guidelines and can be adapted for specific business unit 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

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

8.6 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.

8.7 EMERGENCY ACCESS ARRANGEMENTS

In the event of an emergency, users will need to contact their line management using the contact details contained in their business unit’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.

SECTION NINE

LOGICAL ACCESS CONTROL

9 LOGICAL ACCESS CONTROL

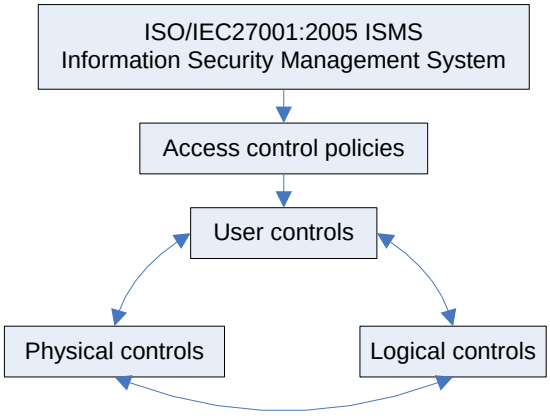
9.1 INTRODUCTION

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 business 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:



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 business unit requirements. Please refer to the LACP guidelines document for further guidance and information.

Logical access controls help protect:

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.

9.2 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):

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

- Network access controls
- Application access controls
- Information access controls
- Privileged use / user access controls
- Encryption techniques
- External access requirements e.g. VPN, 3rd party access etc.

9.3 RESPONSIBILITIES

9.3.1 USER'S RESPONSIBILITIES

a. 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.

b. 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.

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

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

e. 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')

f. There are some special / privileged users who have extra responsibilities:
   - Those users who are responsible for managing applications (application owners / custodians / administrators) on behalf of their business units, shall

control access and usage of such applications and associated business unit information,

- System administrators 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

9.3.2 MANAGER'S RESPONSIBILITIES

a. 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.

b. 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.

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

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

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

f. 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.

g. 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 business unit requirements

h. To define the role of their staff and ensure that the work they do is in line with any relevant council policies

i. To ensure that any visitors for which they or their staff are responsible for must follow logical access controls in accordance with the guidance found in the LACP guidelines document

9.4 LOGICAL ACCESS CONTROL POLICY GUIDANCE

9.5 ACCESS CONTROLS	General access controls that should be considered
9.5.1.1 ***TYPE***	*9.5.1.2* ***CONTROL DETAILS***
Physical controls - See PACP and its guidelines	
Centralised access management	Authorisation Information classification Management authorise access Access request process
	Authentication – the following points should be considered 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 • 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

9.5 ACCESS CONTROLS	General access controls that should be considered
9.5.1.1 ***TYPE***	*9.5.1.2* ***CONTROL DETAILS***
	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 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 Folder and file permissions
	Management and monitoring Auditing / logging Screen savers / automatic lock outs
Type of users	Privileged Normal Visitors Partners Suppliers Contractors / temporary employees
Types of access	Network access

9.5 ACCESS CONTROLS	General access controls that should be considered
9.5.1.1 ***TYPE***	*9.5.1.2* ***CONTROL DETAILS***
	• Use of Active Directory to authenticate users • Firewalls • Packet filtering • Restricted use of protocols • Detection and monitoring Application access 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. PCs Servers Loaned equipment

9.6 USE OF HARDWARE / EQUIPMENT	Controls and issues around the use of hardware and equipment
9.6.1.1 ***TYPE***	*9.6.1.2* ***DETAILS***
Hardware / equipment controls	Only approved hardware, by Desktop & Infrastructure Services or business unit management, 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

9.6 USE OF HARDWARE / EQUIPMENT	Controls and issues around the use of hardware and equipment
9.6.1.1 ***TYPE***	*9.6.1.2* ***DETAILS***
	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	Loss / theft Unauthorised access Damage Malicious or fraudulent intent

9.7 USE OF SOFTWARE	Controls and issues around the use of software
9.7.1.1 ***TYPE***	*9.7.1.2* ***DETAILS***
Software controls	Only Desktop & Infrastructure Services or business unit 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:

9.7 USE OF SOFTWARE	Controls and issues around the use of software
9.7.1.1 ***TYPE***	*9.7.1.2* ***DETAILS***
	• Limit to one login account • Password protected screen savers • Day-time usage limits, e.g. 07:00 to 19:00 • Password controls • ID controls • RAS controls • 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 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
9.8 GENERAL CONTROLS	General controls that support the controls suggested in this document
9.8.1.1 ***TYPE***	*9.8.1.2* ***DETAILS***
Confidentiality agreements	
Policies	Corporate Information and Security Email and Internet policy Logical Physical Acceptable Usage Password

9.7 USE OF SOFTWARE	Controls and issues around the use of software
9.7.1.1 ***TYPE***	*9.7.1.2* ***DETAILS***
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 TEN

ANTIVIRUS AND SOFTWARE

10 SECTION 10: ANTIVIRUS AND SOFTWARE UPDATES

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.

The ICT Division 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.

10.1 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 anti-virus software. This anti-virus 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 Division 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 Division.

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

10.2 SOFTWARE AND FIRWARE 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 division.

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

10.3 BEST PRACTICES FOR VIRUS PREVENTION:

- Always run the standard anti-virus software provided by the Municipality.
- Never open files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
- 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.
- 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.
- 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.
- 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 business critical files is to compress the file using a file compression utility.
- Never copy download, or install files from unknown, suspicious, or untrustworthy sources or removable media or untrustworthy sources or removable media.
- Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
- Avoid direct disk sharing with read/write access. Always scan any removable media for viruses before using it.
- 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.
- Back up critical data and systems configurations on a regular basis and store backups in a safe place.
- Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

10.4 THE FOLLOWING ACTIVITIES ARE THE RESPONSIBILITY OF THE ICT DIVISION:

- ICT division is responsible for maintaining and updating this Anti-Virus 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.
- ICT Division will keep the anti-virus 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.
- ICT Division 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.
- ICT Division will apply any updates to the services it provides that are required to defend against threats from viruses.
- ICT will install anti-virus software on all desktop workstations, laptops, and servers.
- ICT will assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes.
    - 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.

10.5 THE FOLLOWING ACTIVITIES ARE THE RESPONSIBILITY OF THE USERS

- Users must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.
- Users Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.
- Users who don't employ staff with enough technical knowhow to ensure compliance with this policy should seek the assistance of IT Division to do so.
- Users Departments' compliance with this policy shall be subject to audit.
- All employees are responsible for taking reasonable measures to protect against virus infection.
- Employees must not attempt to either alter or disable anti-virus 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

11 SECTION 11: ICT FAULT REPORTING AND MANAGEMENT

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.

11.1 INCIDENT REPORTING

The ICT division 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 division to enable users to log calls via email.

11.2 INCIDENT TYPES

The ICT incidents shall be classified in as per the following high level categories:

- Security
- Network
- Server
- Software
- Application
- User

11.3 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.

11.4 REPORTING AN INCIDENT

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

11.5 LOGGING OF THE INCIDENT

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

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

11.7 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.

11.8 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 division shall have a maximum of 24 working hours to resolve an incident unless it can be resolved due to hardware replacement or availability of parts.

11.9 INCIDENT REVIEWS

The ICT division 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 TWELVE

BACKUP AND RESTORE

12 BACKUP AND RESTORE

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 business activities in accordance with the Municipality's compliance standards in a manner that:

- Supports the achievement of the Municipality's business objectives and financial soundness.
- Will result in a low risk of non-compliance with the letter and spirit of the compliance laws, rules and standards.

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:

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

.

12.4 KEY OBJECTIVES

12.4.1 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.

12.4.2 BACKUP FREQUENCY

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

Daily Backup	Monday to Friday
Weekly Backup	Every Friday
Monthly Backup	Last working day of every Month
Yearly Backup	Last working day of every year

Full backup will be run on all the above schedules.

12.4.3 BACKUP MEDIA

In order to ensure backup redundancy and quick recovery of data and databases backup shall be made to disk and then to tape on a daily bases. The type makes and capacity of the tapes and disk shall be based on the device used.

12.4.4 OFFSITE STORAGE

The Municipality shall arrange for off-site storage of tapes in an environment that meets the following requirements:

- Fire proof
- Water proof
- Dust proof
- Magnetically shielded

Tapes or backup media shall be moved to the offsite backup every Monday Morning. Monthly backups shall be stored in a secure storage on a third location.

12.4.5 TESTING OF BACKUP TAPES

Backup testing shall be carried out to ensure that a backup has been successful and a restoration option is available. A backup restoration plan shall be formulated by the ICT Division:

- Daily backup tapes should be restored at least twice a year for key financial systems which should include one full restoration.
- Monthly backup tapes should as a minimum be restored once a year for key financial systems.

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.

12.4.6 RETENTION AND DISPOSAL OF MEDIA

The retention and disposal of media shall be as follows:

Backup Type	Retention
Daily Backup	14 days
Weekly Backup	4 Weeks
Monthly Backup	12 Months
Yearly Backup	5 years

As unusable or damaged backup tapes contain sensitive data, they are stripped off the cartridges and destroyed.

SECTION THIRTHEEN

NETWORK MANAGEMENT & PROCEDURE

13 NETWORK MANAGEMENT & PROCEDURE

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.

13.1 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.

13.2 SCOPE

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

13.3 LAN AND WAN GUIDELINES

13.3.1 LAN REQUIREMENTS

- Every device connecting to the Network shall be named in terms of the Naming standards created by the ICT division.
- All computer equipment (network and standalone) must be asset-tagged and registered in the Municipality's asset register.
- 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.
- The centralized anti- virus solution is the only anti- virus software allowed on the network.
- For computers attached to the network, the Systems Management Server (SMS) client and other application clients must be installed on all desktops and laptops.

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

13.3.2 WORKSTATION REQUIREMENTS

- 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.

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

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

13.3.3 SERVER REQUIREMENTS

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

13.3.4 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 established an enterprise anti- virus solution that automatically updates systems on all the Municipality's computers. The products used are approved by the ICT Division and may only be installed and or uninstalled by the ICT Division.

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.

13.3.5 DESKTOP MANAGEMENT

Desktops will be managed using the windows domain controller; automatic updates will be controlled using windows update services.

Systems Management Server (SMS) is the Municipality's network management tool for PCs. A SMS client file must be on all networked computers and servers to provide for remote support. Support includes, but is not limited to, computer maintenance, field support, updates, inventory, security, management, and administration. In order to ensure that SMS functions properly, Windows clients will need to run a login script provided the ICT Division. For local domains, the SMSLS.bat file must be included in the login script for all users. Furthermore, local domains will need to establish a trust relationship with the enterprise domain.

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

VPN benefits include:

- Allowance of administrative access on instructional VLAN
- Extended geographic connectivity
- Improved productivity
- Improved security
- Provision of global networking opportunities
- Provision of broadband networking compatibility

13.3.7 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.

13.3.8 FIREWALLS

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

13.3.9 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 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.

13.3.10 RESTRICTIONS

Users may not run:

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

13.4 SERVER INSTALLATION AND CONFIGURATION

13.4.1 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.

13.4.2 INSTALLATION

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

13.4.2.1 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.

13.4.2.2 ADD-ON/REMOVAL DURING INSTALL

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

13.4.2.3 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 2008 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.

13.4.3 SERVER CONFIGURATION

13.4.3.1 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.

13.4.3.2 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.

*13.4.3.3 **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

13.4.4 WINDOWS 2008 SERVER CONFIGURATION

This section outlines the steps necessary to secure computers running Windows 2008 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 2008 R2 Servers.

*13.4.4.1 **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.

*13.4.4.2 **ACCOUNTS***

13.4.4.2.1 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.

13.4.4.2.2 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.

13.4.4.2.3 Disable Guest Account

By default, the Guest account is disabled on systems running Windows 2000 Server. If the Guest account is enabled, disable it.

13.4.4.2.4 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:

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

13.4.5 ACCESS CONTROL LIST

13.4.5.1 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.

13.4.5.2 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.

13.5 SECURITY

13.5.1 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:

- IPSEC

- DNS
- DHCP
- SNMP
- 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.

13.5.2 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.

13.5.3 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 (! #, ; : …)

13.5.4 ADDITIONAL SECURITY SETTINGS

There is additional security features not covered in this document that should be used when securing servers running Windows 2008. 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.

13.5.5 SERVICE PACKS

13.5.5.1 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

13.5.5.2 INSTALL THE APPROPRIATE POST-SERVICE PACK SECURITY HOTFIXES

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

13.5.6 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.

13.5.7 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.

13.5.8 APPLICATION-SPECIFIC CONFIGURATIONS

13.5.8.1 IIS

- Install on data partition, i.e., D:\, E:\, etc.
- If only using one IP address, make sure to unselect "**Use all assigned IP addresses**."
- Select the assigned IP (do this for both WWW and FTP services options).

- Install the default Web/FTP directories to the data partition (D:\inetpub).
- Review the *IIS Baseline Security Checklist* for any additional steps needed (see Microsoft website)
- Install the *IIS Cumulative Patch*
- Install the *IIS Lockdown Tools*

13.5.8.2 TS (TERMINAL SERVICES)

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.

13.5.8.3 SQL

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

13.5.9 SERVER RECOMMENDATIONS

13.5.9.1 RECOMMENDED APPLICATIONS

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

- Microsoft Windows Server
- Microsoft desktop operating system
- Microsoft Office
- Backup Exec
- Fortinet
- Trend Office scan
- Pastel Evolution

13.6 NAMING STANDARDS

13.6.1 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.

13.6.2 WORKSTATION NAMING STANDARD

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

[**Department] [Machine type] [Make] [Asset number]**

Character Position	Field Width	Field Name	Acceptable Values
1-3	3	Department	100 – Office of the MM 200 - Finance 300 – Corporate Services 400 – Community Services 500- Technical Services
4-7	4	Machine type	LAPTOP DESKTOP
8-9	2	Make	01 – Lenovo 02-HP 03-Dell 04 Clone
10-15	6	Asset number	999999

13.6.3 SERVER NAMING STANDARD

Server names, which are seen and referenced frequently by end-users, need to be less cryptic and more intuitive than workstation names. Server names are composed of four fields, each serving a distinct purpose.

[Site] [Constant] [Function] [Sequence number]

The location is based on the existing DNS site suffix used at each Site, excluding any dashes, and truncated to nine characters. DNS suffixes are available from the ICT division.

The constant is the dash (-), which is used to separate the location and function of each server in the server naming standard.

13.6.4 FUNCTIONAL NAMING TABLE

Functional names are always three characters. The most common are presented in the table below. Additional functional names may be created as necessary but they must be restricted to three (3) characters.

Functional Convention Naming Function

AVU - Anti-Virus Update Server	APP- Application Server
DBS - Database Server	DNS- DNS Server
XCH- Exchange Mail Server	SRV -File and Print Server
PSV -Print Server	ADM- Remote Administrative Management (currently SMS
SQL -SQL Database Server	SMS -SMS Server
WEB- Web Server	SUS- Windows Update Services
DCR – Domain Controller	GIS- Graphical Information Systems Server
DCC- Domain Controller Catalogue	BKP- Backup server
PDC- Domain Controller PDC	

13.6.5 SERVER NAMING TABLE

Server names can vary in length up to 15 characters according to the following table:
[Mun code] [-] [Function] [Server name]

Character Position	Field Width	Field Name	Acceptable Values
1-3	3	Mun Code	First three characters of the municipality's name
4	1	-	Separator-
5-7	3	Function	Function Convention Naming as above
8-15	8	Server name	Unique server name defining it.

13.6.6 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
[Municipality abbreviation] [.] [Local]
E.g. ABC local

External domain
[Municipality's abbreviation] [.] [Gov] [.] [Za]
e.g. abc.gov.za

If the municipality's name is less than 8 characters long then the full name shall be used.

13.6.7 USER NAMING STANDARDS

The naming resolution for the username shall me:
[Surname] [First initial of the name]

If a duplicate name exists then a number sequence will be added at the end of the username.
E.g. Joe Xaba = Xaba the second one will be XabaJ2

13.6.8 EMAIL NAMING STANDARDS

The email address shall be the user's name.surname@externaldomain of the municipality
e.g. joe.xaba@abc.gov.za

13.7 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 division.

13.7.1 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 Division, must weigh security with operational necessities. This section specifies the minimum requirements for securing a Windows operating system. The ICT division 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.

13.7.2 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.

13.7.3 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.

13.7.4 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.

13.7.5 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.

13.7.6 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.

- *The Help Assistant, Guest, and Support_xxxxxxxx accounts should be disabled.*
- *The Administrator account should be renamed to root.*
- *The password of the root account must be changed to 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.

13.7.7 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.

13.7.8 5.3.2.1 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.

13.7.9 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.

13.7.10 ICT ADMINISTRATOR ACCOUNT

ICT will be 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	Enterprise admin	Enterprise Admin, Exchange Admin,

Administrator		domain admin, remote desktop.

13.7.11 MISCELLANEOUS SECURITY SETTINGS

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

13.7.11.1 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.

13.7.11.2 DO NOT AUTOMATICALLY START WINDOWS MESSENGER INITIALLY

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

13.7.11.3 ALWAYS WAIT FOR THE NETWORK AT COMPUTER START-UP AND 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.

13.7.12 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 division.

13.7.13 ACCOUNT MANAGEMENT

Every new user will complete the approved service request form which can be obtained from the ICT division 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.

13.7.14 EXCHANGE 2003 OR LATER

Exchange Outlook Web Access offers similar functionality to Outlook such as shared calendar support and an attractive user interface. As a result, it is unnecessary to create a local domain solely to address Exchange functionality concerns. ICT will ensure that a

digital certificate is installed on the server to ensure secure access into the exchange server remotely via web access.

13.7.15 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.

13.8 6 COMPUTER IMAGING REQUIREMENTS AND PROCEDURES

13.8.1 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.

13.8.2 REQUIREMENTS

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

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

13.8.3 INSTRUCTIONS

The ICT division 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

13.8.4 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

13.8.5 JOINING A DOMAIN

The process of joining a domain from a workgroup will have two effects on the machines or above:
· New user profile will be generated
· Domain administrators' rights on local device will be enabled

The system will be joined into the INSTR 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 FOURTHEEN

RISK MANAGEMENT

14 RISK MANAGEMENT

It is the policy of the Municipality to operate an integrated process for the management of risk and the development of a risk register is a logical starting point in this regard. Using the process outlined in this policy the service1 will take stock of the context of its operating environment, identify key risks, assess the risks and review the service capacity to deal with the risks.

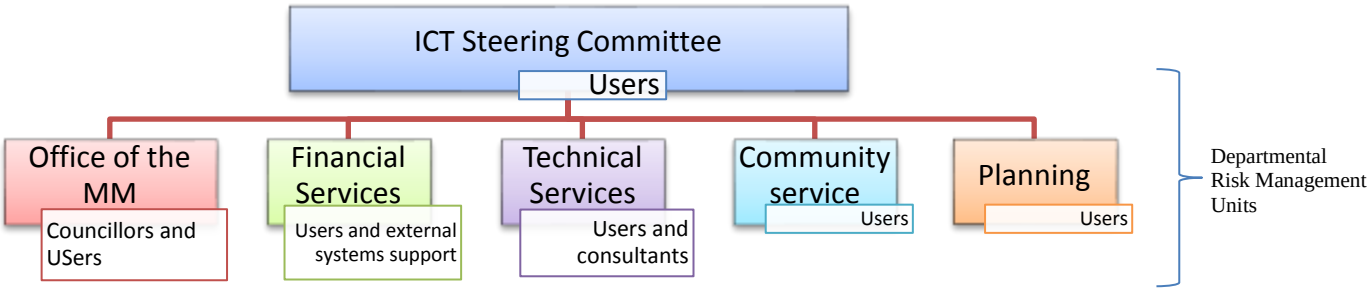
The outcome of this process is the development of a risk register which helps a service to establish a direction for managing its risks. The risk register consequently provides managers with a high level overview of the services' risk status at a particular point in time and becomes a dynamic tool for the monitoring of actions to be taken to mitigate risk.

The risk register is a key example of evidence required in COMSEC audit, Auditor General and MISS

14.1 RESPONSIBILITIES

Risk management is a line management responsibility and consequently the line manager is responsible, in consultation with his/her staff, for the development of a risk register in their area of responsibility. The risk register when complete should be brought to the attention of all employees working in the service in a clear and understandable manner taking into account their level of training, knowledge and experience. A critical part of the risk register is an action plan to address the additional controls identified as required to reduce the risk to an acceptable level. Additional controls (actions) identified as being required that cannot be managed at the service level at which they have been identified should be referred to the next level of management in order that decisions can be taken to manage them. Such decisions may involve the allocation of required resources, the provision of required authority or to escalate the action to a higher level of management. At any stage in the process it may be decided to 'live with' or accept a certain level of risk as it is acknowledged by the Municipality that not every risk can be eliminated, for practical or other reasons.

A risk that cannot be completely eliminated must, nevertheless, be recorded in the relevant risk register along with a list of controls to be in place to reduce the risk to an acceptable level. These accepted risks will be monitored by the relevant service on a regular basis. Risk Registers will capture risk information from the "bottom up" within each Department. The risk register will be a primary tool for risk tracking, and will contain the overall system of risks, and the status of any risk mitigation actions. (See Figure 1)



14.2 ROLES OF DEPARTMENTAL RISK MANAGEMENT UNITS

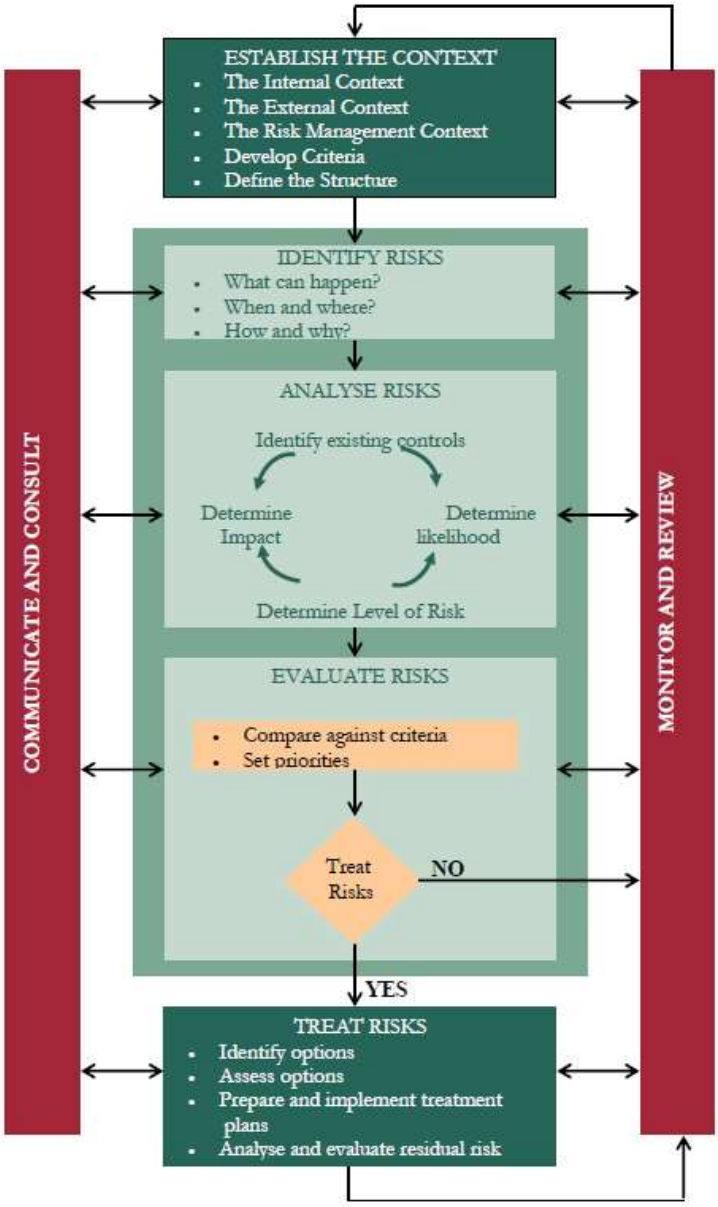
The principal purpose of the Departmental Risk Management unit, where available, is to facilitate, support and advise the Head of Department and users in relation to the management of risk. It is not their responsibility to manage risks identified within a service. The management of risks is a line management function and responsibility.

14.3 ROLE OF THE ICT STEERING COMMITTEE

The role of the ICT steering with regard to this process is to offer support, advice and facilitation as is required. This is of particular importance in the instance where there are no Departmental Risk Management Units. The ICT Steering committee will also offer advice to the Departmental. The Committee also has a role in the provision of independent assurance in respect of the risk register process.

The Committee shall review the Departmental risk registers in every sitting and shall observe the recommendations and escalate them for auctioning to MANCO with its own recommendations and proposals.

14.4 OVERVIEW OF THE PROCESS FOR THE DEVELOPMENT OF A RISK REGISTER



14.4.1 DEVELOPING DEPARTMENTAL RISK REGISTERS

Figure 3. Steps in the Development of a Service Area Risk Register

14.4.2 PREREQUISITES TO UNDERTAKING THE PROCESS

14.4.2.1 AVAILABILITY OF RISK EXPERTISE

It is accepted that the extent of the risk expertise required to support the process is variable throughout the Municipality. The profile of available risk expertise essentially falls into three broad categories.

1. Departments which have internal access to risk staff who would be familiar with and have the experience required to fully support the process from the outset pending orientation to the standardised process and tools to be used.

2. Departments which have risk staff that are not familiar with nor have the experience to fully support the process from the outset and will require training in preparation for supporting development of the register and recourse to expertise in the form of coaching throughout the process.

3. Departments which have no access to risk expertise and will need access to this externally.

14.4.2.2 USE OF APPROVED SUPPORT MATERIALS AND TOOLS

The Municipality has approved a number of documents and tools to support this process in a uniform and standardised manner. It is essential that all areas who undertake the process of developing risk registers use these materials and tools in a consistent way. This document and other support materials are reviewed regularly and it is essential that the latest version of these is used when undertaking the process. The tools can be obtained from the ICT division or on the Municipality's shared folder.

14.4.2.3 COMMITMENT AND OWNERSHIP

This is critical to the success of the process. There needs to be visible commitment of the senior manager in the area in which the process is being undertaken. This commitment must be communicated and support gained from the service managers who, along with their staff will be participating in the process.

As the management of the completed register(s) will lie with the Head of Department to which they related, it is essential that they take ownership of the development process from the outset. It is the role of the risk staff to support the process and to advice in relation to maintenance of the completed register and not to manage the risks identified.

14.4.2.4 ADMINITRATIVE SUPPORT

The process of developing risk registers requires support of an administrative nature e.g. organisation of workshops, co-ordination of the process, point of contact within area etc. A person of sufficient seniority needs to be designated to support the process.

14.4.3 STEPS TO BE FOLLOWED IN DEVELOPING A RISK REGISTER

14.4.3.1 STEP 1: RISK REGISTER AWARENESS AND ORGANISATIONAL READINESS

• **Initial planning by Service Area Manager and Risk Management Support Person**

The Head of Department should meet with the Risk Management support person. The purpose of this meeting is to ensure that the Head of Department has an overview of the risk management process and to discuss and agree the development of risk registers in their area of responsibility. At this meeting the each business unit falling under that Department should be present; the lead person should be identified in this meeting.

• **Describe in detail the accountability structure for the management of quality and risk.**

It is key critical to spend time at the outset in describing the accountability structure for the management of quality and risk within the Department. This is required as the actions required to mitigate risks identified at any level may not be within the control of the manager at that level and may require notification and escalation to a more senior level of management for action. The lines of responsibility need to be clearly defined on the principles of line management.

• **Describe the Department's internal, external and risk management**

The context in this regard is dependent on those factors which impact on the particular business unit where a risk register is to be developed.

The internal context will be the context of the business units Operations. The external context will include any legislation and political mandates.

Ensure appropriate communication and consultation throughout the development process.

Good communication is paramount in developing a 'culture' where positive and negative dimensions of risk are valued. Engaging with others can help to embed risk management as a normal part of the way services operate. Communication efforts must be focused on consultation, rather than one way flow of information from decision makers to stakeholders. Initial communication will commence with the organisation and delivery of the risk register briefing meeting with the management team, service leads and other relevant staff.

The purpose of this briefing is to outline the overall process to be undertaken, their role in the process and the benefits of the process to them.

14.4.3.2 STEP 2: MEET WITH SERVICE LEADS AND THEIR MANAGEMENT TEAMS

The Risk Management support person should meet with each service nominated lead and other key members of their management team prior to their service workshop. The purpose of this meeting is to:

• Provide an overview of the purpose of the risk management process and the process of the workshop;
• Stress the importance of establishing the Service context (external, internal, risk management)

It is important to ensure that high quality information/data is used in identifying risks. The Head of Department of the service in which the risk register is being developed should ensure that a process is undertaken to identify risks from any information source available.

14.4.3.3 STEP 3: CONDUCT SERVICE RISK IDENTIFICATION WORKSHOPS

The Risk Management support person facilitates the risk identification workshop(s) with a cross section of employees relating to the service in which the risk register is being developed.

At the workshop(s) the Risk Management support person should:

- Give an introduction to Risk Management to cover why risk management is important, what are the benefits of risk management and an overview of the risk management process. Take time to explain this objective of the workshop to those attending i.e. to use their knowledge of the service to identify those issues that might pose risk.

- Conduct the first break out session, during this the attendees work individually to brainstorm all the issues they perceive pose risk to (a) day to day operations, (b) employees and (c) the organisation. Issues identified are recorded on mind map or Visio and gathered by the Risk Management support person and displayed on the wall under the headings of (a) day to day operations, (b) employees and (c) the

organisation. It is a good idea to project the minds map on the projector. The must be grouped and themed together based on similarity. If a number of departments are attending at the workshop ensure that they identify their department on each branch in the mind map or alternatively provide each department with different a different mind map. This is critical as the mind map will be used to develop the risk list (and the subsequent assessment) for creating the departmental risk register.

- Take a sample number of issues identified as a result of this process (it will not be possible to review all the issues identified at the workshop) and through a process of discussion with those attending describe the risks associated with these issues. The risks should be described using the Impact, Causal Factor & Context (ICC) approach. The risks described will be used for the next break out session where attendees will work in groups.

- After the attendees have described a number of risks (at least one per group), the Risk Management support person should use one of these to demonstrate how to assess a risk using the Municipality's Risk Assessment Tool. As part of this demonstration the Risk Management support person should use the risk assessment exercise sheet to step through the process.

- Conduct the second break out session, during this attendees work in groups to take a number of the risks identified and risk assess each of the risks. The risk assessment exercise sheet and the Municipality's Risk Assessment tool should be used by the groups in this exercise.

- After the second breakout session the Risk Management support person outlines the next stages in the risk register development process and thanks the attendees for their valuable input and contribution to the workshop. All employees present at the workshop should fill out an evaluation form so as to evaluate the degree to which the objectives of the workshop were achieved.

14.4.3.4 STEP: 4. DEVELOPMENT OF RISK REGISTERS WITH SERVICE MANAGEMENT TEAMS

Initial post workshop meeting

This is ideally held directly following the workshop. The service lead should then convene the services management team or a smaller group of senior employees if a formal management team is not in place. This group will consider the issues identified from the workshop and consider any other sources of risk information with a view to identifying the risks to the service. The local Risk Management support person should provide support and advice to this group. The outcome of this meeting will be a draft risk list (using the ICC approach to risk description which

should then be circulated to the members of the group for final consideration. It may also be decided to circulate it to other persons who the group may wish to consult.

Subsequent meetings to complete the Risk Register

The purpose of subsequent meetings is to agree the risk list and to complete the risk assessment for each risk identified. Each risk identified should be documented on a Risk Assessment Form.

(**Hint:** It is recommended that prior to the first of these meetings that the risks on the draft risk list are copied and pasted (one per form) onto blank Municipality Risk Assessment Forms. At the meeting a soft copy of these can be projected on a screen and any amendments/additional information inputted directly onto them at the meeting).

- Consider each of the risks separately, describe and document on the risk assessment form the impacts/vulnerabilities of the risk. (Note: these are the impacts and vulnerabilities that attach to the risk in general and are not an indication of impacts/vulnerabilities existing within the service). The documenting of these here will assist with both the impact assessment process and with identifying the types of impacts/vulnerabilities which need to be controlled i.e. assist in identifying additional controls required.

- For each risk agree what controls are required in order to manage the risk effectively. A combination of different types of control may be required. When trying to think of what controls should be

  In place it is often useful to consider these in a logical manner e.g. starting with policy and procedures, (clinical and non-clinical), the actions undertaken to implement these (training, education, resources, use of physical environment etc.), through to monitoring and evaluation to ensure compliance.

- Identify and document which of the required controls are currently in place i.e. existing controls.

- Consider the adequacy of the existing control measures and their effectiveness in minimising risk to the lowest reasonable practicable level.

- Rate the risk by assessing the likelihood and impact of the risk and plotting these scores on the Municipality's Risk Matrix. In rating the risk, account must be taken of the adequacy the existing controls that are in place. The municipal's Risk Assessment Tool must be used for the process of rating the risk.

- Depending on the initial risk rating and the adequacy of the existing controls in place an evaluation must be made on whether to accept the risk or that additional controls or other actions are required to mitigate the risk i.e. risk treatment.

- For those risks deemed acceptable a process needs to be put in place to monitor and review the risk. The review date and the risk status of 'monitoring' need to be documented on the risk assessment form.

- For those risks that are not deemed acceptable, the team need to consider the options available to them to treat the risk e.g. those controls that were identified at the outset as necessary to manage the risk and that do not currently exist. It is important when documenting the actions required to ensure that they are explicit to others when read as some actions may need to be escalated to a manager outside the service where there may not be the same level of implicit understanding.

- To ensure that the additional controls identified in this step of the process will adequately mitigate the risk, the group should re-rate the risk taking account of a situation where the additional controls would be in place. This should be done using the Municipal Risk Assessment tool and documented on the risk assessment form.

- After the additional controls required have been agreed the team should identify and assign a person who has responsibility for ensuring that these additional controls are implemented. For those additional controls that can be managed within the service the name of the person within the service who has been assigned responsibility to action the additional control should be captured on the risk assessment form. The Service Lead(s) need to arrange a meeting with the person's assigned responsibility to manage the additional control(s). The purpose of this meeting is to agree the action plan(s) required and to agree the due date for implementation. The agreed due date will have to be documented on the relevant risk assessment form. **Note:** For this meeting it is important to have an up to date soft copy of the relevant service risk assessment forms so that any changes made at the meeting can be done on the day. It is important that one person is assigned responsibility to co-ordinate the management of the additional control (action).In the absence of an ICT system it is important that those persons who have been assigned responsibility for the additional controls are given a copy of the completed risk assessment form. This is important as the responsible persons will have to provide an update on the status of these additional controls on a 3 monthly basis.

- For those additional controls that are identified as not within the span of control of the service to implement the action should be escalated to the person responsible at the next level of management e.g. Head of Department/ The Municipal Manager /ICT Steering Committee. The name of the relevant senior manager to whom the action is being assigned should be captured on the risk assessment form. In the

absence of an ICT system it is important that those persons who have been assigned responsibility for the additional controls are given a copy of the completed risk assessment form. This is important as the responsible persons will have to provide an update on the status of these additional controls on a 3 monthly basis.

- Each of the risks should be assigned a risk status. With regard to the risk status the options available are:
  - Open, i.e. additional controls have been identified as necessary
  - Monitor, i.e. existing controls are deemed adequate to manage the risk but these need to be periodically reviewed.
  - Closed, i.e. that the risk no longer exists e.g. where an unsuitable premises is replaced by a suitable one.
- Categorise the type of risk by assigning a primary, secondary and tertiary risk category from the Risk Categorisation In categorising risk the primary category should link to the primary area of impact. The secondary and tertiary categorisation will flow naturally from this choice and taking account of the overall risk description. This categorisation should be documented on the risk assessment form.

- At this point ensure that all remaining information required on the form has been filled in for a description of the information required for each field)

Hint: The time taken to complete the assessment of the first risk with the team will be considerable. As the group gets more familiar with the process the time taken will shorten. This can be accelerated further when members of the group are confident with the process by agreeing to divide the remaining risks to be assessed between the members of the group (email the forms to members) and for each of the members to work between meetings to complete a draft assessment of the risks emailed to them. The drafted risk assessments should be emailed back to one nominated person before the next meeting. The nominated person saves all draft risk assessments and brings these on a laptop for discussion and agreement with the group. The focus of the next meeting is therefore around reaching consensus on each drafted risk assessment form rather than working from scratch with each risk.

- At the end of this step in the process the service will have a complete risk assessment form for each risk identified for their service. These forms collectively represent the services risk register and are in a format which can be inputted directly onto the Municipal ICT Risk Register when available. In the absence of the Municipal ICT Risk Register the persons responsible for the additional controls will also have received a copy of the completed risk assessment forms to enable them to provide a 3 monthly update to the Head of Department (HOD).
- If an improvement plan is not required the agreed timeframe for action should be documented and attached to the risk assessment form. If an improvement plan is required this should be developed in accordance with the FOCUS – PDCA improvement model. An outline of the FOCUS - PDSA cycle can be obtained.

At this stage in the process each of the services within the Service Area will have a completed risk assessment form for each risk identified in their services.

The assessed risks can be categorised as follows:

1. Those risks that require monitoring and review within the service they were identified i.e. risks where no further additional control(s) have been identified as necessary.

2. Those risks where the additional controls(s) can be managed at local level and the responsibility for managing those additional control(s) has been assigned to person(s) within the department.

3. Those risks where there is a combination of escalated and locally managed additional control(s). **Note:** It is important for those risks that have a combination of local and escalated additional controls that any changes to the risk assessment form need to be notified to the coordinator of this step in the process so as to ensure that the Head of Department has the most up-to-date risk assessment form on their risk register.

4. Those risks where the additional control(s) cannot be managed at local level and these have been identified as requiring escalation up to the ICT Steering Committee.

*14.4.3.5 **STEP 5: DEVELOPMENT OF THE DEPARTMETNAL RISK REGISTER***

The Head of Department convenes a separate meeting with each of the service leads and the person assigned responsibility to co-ordinate this step of the process. The purpose of this meeting is to evaluate and agree with the service lead the additional controls identified as being the responsibility of the Service Area Manager.

At this meeting the Head of Department can:

- Agree to accept responsibility for the additional control(s) or consider assigning the additional control(s) required to a relevant senior manager on their management team or;

- Where the additional control(s) required is outside of the control of the department, they can escalate the additional control(s) up to I CT steering Committee or;

- Modify or add additional control(s) and accept responsibility for this, assign it to a relevant manager on their management team or escalate to the ICT Steering Committee or;

- Where the Head of Department is notified of a risk from one service that they feel has an impact on all services or where the HOD has been notified of the

same/similar risk from all or a number of services or where a risk identified in one or more services impacts on other groupings the following applies:

Aggregation of same/similar Risks

The HOD creates a new risk onto the Service Area risk register and then identifies the additional control(s) and person(s) responsible required to manage the risk. The HOD may decide to assign responsibility of the additional control to a member of his/her management team or they may decide to escalate relevant additional control(s) up to the ICT Steering Committee for action.

Following this the HOD needs to notify the manager(s) where the original risk was identified and advise them that he/she has created a new risk on his/her risk register and that there is still a need for the manager(s) to manage and monitor the original risk at a service level and to inform the HOD of any change in circumstances.

Finally the HOD needs to notify the Service Leads (who have **not** identified this as a risk in their service) that he/she has created a new risk on their risk register and that there is a need for the service lead(s) to create a risk on their risk register and to manage and monitor this risk at a service level and to inform the Service Area Manager of any change in circumstances.

NOTE: For this meeting it is important to have an up to date soft copy of the relevant service Risk assessment forms so that any changes made at the meeting can be done on the day.

Following on from this meeting the HOD should meet with his/her management team members who have been assigned responsibility to manage the implementation of the additional control(s) to discuss and agree the risk treatment plans. Risk Treatment plans should include:

- Risk reduction/additional controls required
- Resource requirements
- Timescale for implementation, review date, completion date.
- Performance measures
- Reporting and monitoring requirements.

The risk treatment plan should be documented and attached to the risk assessment form. It might be
useful to consider the Plan, Do, Check, Act (PDCA) Cycle for this purpose. An outline of this process can be obtained.

The escalation of additional controls to the ICT Steering Committee Risk Register.

The process as identified above needs to be repeated with the ICT Steering Committee and the
HOD in his/her area of responsibility in the department .The escalations of additional controls to the relevant ICT Steering Committee risk register
.

14.4.3.6 STEP 6. SIGN OFF AND HANDOVER

The purpose of this stage is to conduct a final meeting with the Heads of Departments of those areas in which the workshops took place and in order to

- To sign off the registers
- To present feedback from the evaluations carried out to date
- To advice on the business process for using the registers as a dynamic management tool to manage risk
- To receive any other feedback that will inform future processes in other departments.

Updating Risk Registers

Until the Municipality's ICT Risk Register System is implemented in your area it is vital to have an agreed
manual process in place for updating the registers at all levels in the Service Area. In the absence of an ICT risk register system a possible interim process for updating risk registers is as follows:

- At stage 4 in the process the Grouping/Directorate/Service Lead will have already given a copy of the completed risk assessment forms to those persons assigned responsibility for the additional controls. On a regular basis e.g. 3 monthly, ICT Steering Committee/HOD's will send an email together with a blank update form to those responsible persons and request an update by an agreed date.

- The relevant responsible person(s) will complete the update form(s) and email back to the ICT Steering Committee/HOD's.

- Steering Committee/HOD's will gather all the update forms, check for completeness and attach the relevant update forms to the appropriate risk assessment form(s).

- The above process should be repeated regularly e.g. every 3 months until the ICT risk register is in place.

14.4.3.7 MONITOR AND REVIEW

The risk assessment process should be seen as a dynamic process with the adequacy of the control measures subject to continual review and monitoring and revised where necessary. In general terms monitoring will be one of three types:

1. **At service level**
    - **I.** Monitoring of risks
    - **II.** Identification of new risks

Within any service new risks are likely to emerge from time to time; these are likely whilst operating in an environment of limited resources, changing work environment e.g. regulatory, management, technological etc. The ICT Steering Committee must be aware of such issues which may impact on it and on a continuous basis be reflecting on sources of risk information.

Any new risk identified should be included on the risk register following assessment and the identification of actions required in the same way as those that were identified through the initial risk register development process.

I. Re-assessment of existing risks

It is good practice to review the risk assessment annually taking account of any new controls that have been put in place since the original assessment. This will allow for a re-prioritisation of the risk list thereby focusing the efforts of the service to address those risks that are most pertinent to the service .When re-assessing existing risks, services should compare the risk rating from the re-assessment with the risk rating of the original assessment. If the reduction (or maintenance in certain circumstances) of risk levels is not as anticipated in the original assessment, then they need to check why i.e. have the additional controls been effectively implemented? If they have why are they not reducing the rating? Are they the right controls and if not is there a need to revisit and enhance the control measures?

2. **At Service Area Level**

In the same way as risks are monitored within services, risks should be monitored at a Service Area
Level as outlined above:

a. Monitoring of actions arising from risks identified at Service Area Level
b. Monitoring risks
    i. Identification of new risks
    ii. Re-assessment of existing risks

3. **Monitoring for independent assurance**

From a governance perspective it is essential that not only to demonstrate that services have conducted a proactive risk identification process but also to be able to demonstrate that the process was robust and that it has resulted in a positive effort to reduce risk.

a. Integrity and effectiveness of the process

The integrity of the process is governed by the use systematic application of this guidance and the associated tools (including involvement of relevant stakeholders). The on-going management of the risks identified by this process can be audited using the audit facility inherent in the ICT Risk Register thereby making it a key tool for the monitoring of improvement actions identified as required for a service.

b. Linkages with other sources of risk information

As the risk register is a repository for risk identified from a wide variety of sources it is essential that evidence is available that the services efforts to identify risk go beyond the workshop. This will ensure that risks not identified at the workshop can be included in the risk register or that risks identified at the workshop can be validated further.

SECTION FIFTHEEN

PRIVACY

15 PRIVACY

15.1 PRIVACY

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 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 Municipal Manager management reserves the right to examine email, personal files and other information stored on its equipment.

15.2 DATA PRIVACY

All data is sensitive to some degree, and the degree of sensitivity is unique to each business information area. Users are responsible for the security and privacy of printouts and hard copies of the Municipality's information. The following data is deemed confidential at differing levels as specified:

DATA PRIVACY		
Business Information Area	**Type of data**	**Level of Privacy required**
Council Matters	Reports, Agenda, Minutes	Internal - Confidential
	Resolutions, By-Laws	Public-External
Administration	Reports, Agenda, Minutes, Correspondence, Contracts	Internal - Confidential
	Resolutions	Internal
Income	Debtors master records, transactions, balances	External - Internal
Expenditure	Creditors master records, transactions, quotes, tenders	Internal - Confidential
	Requisitions, Orders, Invoices, GRVs	Internal
	Awarded Tenders and orders	Public - External

Financial	Financial Statements [I&E, B/S]	Public
	Management Accounts, Working Papers	Internal
Projects	Projects Master, Project Management	Internal
Human Resources	All activities and data, work standards and leave records	Internal
	Payroll, personnel details, appraisals, succession plans, training	Confidential
Information Tech	Source Code, System Parameters, Passwords, PINs	Secret

Based on the level of privacy deemed to be required above, the following guidelines apply:

Class of data	**Examples**	**Storage**	**Transmission**	**Destruction**	**Systems applicable**
Public	Public service info.	WWW server, Backup media labelled and stored safely. Scan for viruses	Unconditional	None	WWW services
External	Project Data. Macro-Economic Data , Income Base Data, Map Data	File & App Server Backup Media labelled and stored safely. Scan for viruses , monitor data integrity regularly	Stipulate what info. may be shared with business partners under a contract. Encrypt if transmitted via Internet		Admin Finance Technical GIS
Internal	Reports, meeting minutes, customer details	As per External	Conditional under the approval of MANCO. Encrypt if transmitted via Internet	None	Admin Finance Technical, GIS Personal
Confidential	Salaries info, sensitive data, contract information, Legal Proceedings	As per Internal plus hard copies to be stored under lock and key	Conditional with EXCO approval Passwords to be encrypted. Strong encryption required for Internet transmission.	Documents shredded. Backup tapes and diskettes destroyed.	Salaries & wages HR, Personal
Secret	Source	As per	As per	As per	IT

	Code, Security Tables Pins and Passwords	Confidential plus stored in encrypted format or on removable disks.	Confidential. Disclosed only under the circumstances of a Disaster Recovery or Business Continuity with the authority of EXCO	Confidential.	

Users should be aware that ICT personnel who operate and support the electronic communications, network infrastructure, systems and data need to monitor transmissions from time to time, or inadvertently observe certain critical information during data restores or similar. This policy provides that these personnel are not permitted to see or read the contents intentionally, or disclose or use what they have seen, read or heard unless instructed otherwise by the MANCO. ICT Service Providers and or employees will sign a confidentiality agreement to this effect.

15.3 LIMITED WARRANTY

The Municipality takes no responsibility and provides no warranty against the non-delivery or loss of any files, email messages or data, nor does it accept any liability for consequential loss in the event of improper use or any other circumstances.

In general, it is inappropriate use to store and/or give access to information on the Council's computing and networking facilities that could result in legal action against the Council.

15.4 APPROPRIATENESS

This policy spells out what users may or may not do on the various components of the ICT resources of the Council.

The Council's computing and networking facilities must not be used for the transmission, obtaining possession, advertisement or requesting the transmission of objectionable material. Objectionable material is defined to include:

- Pornography, erotica or nudity of any kind
- any article which promotes or incites crime, violence, racial disharmony
- Any article which describes or depicts in a manner likely to cause offence to a reasonable adult e.g. torture, bestiality, use of violence in sexual conduct etc.

The use of the systems and equipment is inappropriate when that use:

- Compromises the privacy of users and their personal data.
- Constitutes a danger to any person's health or safety.
- Damages the integrity of a computer system, or the data or programs stored on a computer system.

- Disrupts the intended use of system or network resources.
- Wastes resources that are needed for business use (people, network bandwidth, CPU Cycles, etc.)
- Uses or copies proprietary software when not authorised to do so.
- Uses a computer system as a conduit for unauthorised access attempts on other computer systems.
- Consists of unauthorised and excessive snooping, probing or otherwise connecting to a node or nodes in a manner that is deemed not to be of an authorised nature.
- Results in the uploading, downloading, modification or removal of files on any node in the network for which such action in not authorised.
- Uses the mail system to impersonate another user
- Uses Council time and resources for personal gain, illegal activities, recreation
- Theft or copying electronic files without permission.
- Sending or posting Council [external – confidential] files outside the Council to unauthorised designations.

Employees found abusing the privileges granted to them will be subject to monitoring of their activity and disciplinary action, ranging from verbal warnings to termination or legal prosecution.

SECTION SIXTEEN

MUNICIPAL WEBSITE

16 MUNICIPAL WEBSITE

The Municipal website is all about getting the Municipality to speak about itself – to tell its customers (e.g. citizens, investors, tourists) what it does, what services it offers, etc. It is probably one of the single largest communications exercises ever undertaken by the Municipality.

The municipal website shall be an integral part of a municipality's communication infrastructure and strategy. If managed effectively, it allows easy access to relevant information, serves as a tool for community participation, improves stakeholder involvement and facilitates stakeholder monitoring and evaluation of municipal performance.

16.1 RELEVANT LEGISLATION

The role of municipal websites, as platforms for information dissemination, participation and disclosure has been significantly catered for in various pieces of legislation, including:

- The Local Government Municipal Systems Act No 32 of 2000 ("the Systems Act");
- The Local Government Municipal Financial Management Act No 56 of 2003 ("the MFMA"); and
- The Municipal Property Rates Act, no 6 of 2004 ("the MPRA").

Legislation	Requirements
Municipal Systems Act	Section 21 A of the Systems Act states: Documents to be made public (1) All documents that must be made public by a municipality in terms of a requirement of this Act, the Municipal finance Management Act or other applicable legislation, must be conveyed to the local community: (a) by displaying the documents at the municipality's head and satellite offices and libraries; (b) by displaying the documents on the municipality's official website, if the municipality has a website as envisaged by section 21 B; and (c) By notifying the local community, in accordance with section 21, of the place, including website address, where detailed particulars concerning the documents can be obtained.

	21B. Official website.—(1) Each municipality must— (a) establish its own official website if the municipality decides that it is affordable; and (b) Place on that official website information required to be made public in terms of this Act and the Municipal Finance Management Act.
	2) If a municipality decides that it is not affordable for it to establish its own official website, it must provide the information in terms of legislation referred to in subsection (1) (b) for display on an organised local government website sponsored or facilitated by the National Treasury.
	(3) The municipal manager must maintain and regularly update the municipality's official website, if in existence, or provide the relevant information as required by subsection (2) 57(I) (h) of the Municipal Systems Act states that performance agreements for Section 57 Managers must be on the Website1

Legislation	**Requirements**
Municipal finance Management Act	Section 75 of the MFMA requires that the municipalities place key documents and information on their website, including the IDP, annual report, the annual budget2, adjustments budgets and budget related documents and policies3.
	75. (1) The accounting. officer of a municipality must place on the website referred to 1 0 in section 21A of the Municipal Systems Act the following documents of the municipality: ▪ The annual and adjustments budgets and all budget-related documents: ▪ All budget-related policies: ▪ All performance agreements required in terms of section *57(* I *) (h l* of the Municipal Systems Act: ❖ all service delivery agreements; ❖ all long-term borrowing contracts; ❖ all supply chain management contracts above a prescribed value: ▪ □n information statement containing a list of assets over a prescribed value that have been disposed of in terms of section 14(2) or (4) during the previous quarter: ▪ Contracts to which subsection of section 33 apply, subject to subsection *(3)* of public-private partnership

	agreements referred to in section *110:* ▪ all quarterly reports tabled in the council in terms of section *52:* ▪ and any other documents that must be placed on the website in terms of this Act: ▪ Any other applicable legislation, or as may be prescribed. (2) A document referred to in subsection (I) must be placed on the website not later *30* than five days after its tabling in the Council or on the date on which it must be made public, whichever occurs first.
	Advertise and invite representations on any draft resolution on the proposed rates and taxes on its website and public libraries, as required by Section 22 of the MFMA and Section 21 A of the Systems Act.
	Copies of the draft and final Medium Term Revenue and Expenditure Framework / (i.e. Municipal Budgets) in the prescribed format as per Section 17 of the Local Government: Municipal Finance Management Act, 2003 with the following supporting documents: (a) Draft resolutions- (i) approving the budget of the municipality; (ii) imposing any municipal tax and setting any municipal tariffs as may be required for the budget year; and (iii) approving any other matter that may be prescribed; (b) measurable performance objectives for revenue from each source and for each vote in the budget, taking into account the municipality's integrated development plan; (c) A projection of cash flow for the budget year by revenue source. broken down per month; (d) any proposed amendments to the municipality's integrated development plan following the annual review of the integrated development plan in terms of section 34 of the Municipal Systems Act; (e) any proposed amendments to the budget-related policies of the municipality: (f) particulars of the municipality's investments; (g) any prescribed budget information on municipal entities under the sole or shared control of the municipality; (h) particulars of all proposed new municipal entities which the municipality intends to establish or in which the municipality intends to participate: (i) Particulars of any proposed service delivery agreements. including material amendments to existing service delivery agreements;

	(j) particulars of any proposed allocations or grants by the municipality to- (i) other municipalities; (ii) any municipal entities and other external mechanisms assisting the Municipality in the exercise of its functions or powers: (iii) any other organs of state; (iv) any organisations or bodies referred to in section 67(1) : (a) (k) the proposed cost to the municipality for the budget year of the salary, allowances and benefits of- (i) each political office-bearer of the municipality; (ii) councillors of the municipality; and (iii) the municipal manager, the chief financial officer, each senior manager of the municipality and any other official of the municipality having a remuneration package greater than or equal to that of a senior manager; (l) the proposed cost for the budget year to a municipal entity under the sole or shared control of the municipality of the salary, allowances and benefits of- (i) each member of the entity's board of directors: and (ii) the chief executive officer and each senior manager of the entity; and (m) Any other supporting documentation as may be prescribed.
Municipal Property Rates Act	Public notice of valuation rolls 49. (1) The value of a municipality must submit the certified valuation roll to the municipal manager, and the municipal manager must within 21 days of receipt of the roll- *(a)* publish in the prescribed form in the provincial *Gazette,* and once a week for two consecutive weeks advertise in the media, a notice- (i) stating that the roll is open for public inspection for a period stated in the notice, which may not be less than 30 days from the date of publication of the last notice; and (ii) inviting every person who wishes to lodge an objection in respect any matter in, or omitted from, the roll to do so in the prescribed manner within the stated period; *(b)* disseminate the substance of the notice referred to in paragraph (*a)* to the local community in terms of SECTION 4 of the Municipal Systems Act; and *(c)* Serve, by ordinary mail or, if appropriate, in accordance with section 115 of the Municipal Systems Act, on every owner of property listed in the valuation roll a copy of the notice referred to in paragraph *(a)* together with an extract of the valuation roll pertaining to that owner's property. (2) If the municipality has an official website or another website available

16.2 WEBSITE ADMINISTRATOR RESPONSOBILITIES

The Municipal Manager shall appoint a website administrator who will be responsible for the following:

- Educating Authors and Customers
- Generating Log Reports
- Publishing & Managing Content
- Securing the Website and Servers
- Managing user/group accounts
- Interacting with clients
- Monitoring/Tuning server Performance
- Server-side Programming / ASP or PHP
- Client-side scripting / DHTML and JavaScript
- Templates creation for Authors
- User & Technical Documentation
- Up skilling & Following technology
- Website promotion

16.3 WEBSITE AUTHORS RESPONSIBILITIES

An Author is any one of who will actually be responsible for collating content and publishing it in some form on your web server/s.

Anyone can supply content, but not everyone is likely to be actually publishing as such. In a large organisation, people are often assigned to the role of content authoring, or administering.

The more a Webmaster can pass on to these distributed web owners or custodians, the easier it is for them in turn to pass on knowledge or skills to staff within their team, department or workgroup thus freeing up more time for the Webmaster to focus on the other tasks listed on this page.

Authors will generally need some knowledge of HTML even if they are mainly using a WYSIWYG editor to publish content. With a background in HTML an Author is more likely to be able to fix a problem page themselves, rather than pester the Webmaster for support.

The Head of Department shall appoint Web Authors, who must: identify information about their department/branch that should be on the portal; write content and make sure it’s up to date; and make sure they send the content to the correct custodian for approval.

The Responsibilities of the website author shall be:

- Identify information about their departments that should be on the website
- Stratergise how information should be presented on the website
- Make sure that their departmental/branch information is always up to date.
- Write the content in keeping with the government communicators guide

- Comment on the content of other Web Authors and Custodians when asked to

The following rights will apply to Web Authors

- Enter Content
- Decide where it should appear on the website
- Send the content for authorisation to the appropriate Custodian

The following guidelines shall be used when selecting a Web Author
Each department is responsible for choosing its own Web Authors. Departments will ideally end up with many Web Authors, with each one responsible for a particular area. In the beginning, though, departments will probably have to start with fewer Web Authors, while everyone is getting used to content Management system and the website.

Those people should:
• Have worked with publishing information, or at least understand information and how to present it.
• Have an in-depth understanding of the department
• Have good planning and organisational skills.
• Ideally be proficient in two of the three official languages of Kwazulu/Natal.
• Be customer driven, i.e. able to focus on what users want.
• Have good writing skills

16.4 WEBSITE CUSTODIANS RESPONSIBILITIES

The position of Custodian is very important and there is a high level of trust vested in the position: Custodians can approve content anywhere on the portal (guided by any departmental or other policies set up to constrain which content areas they may operate in).

RESPONSIBILITIES OF THE CUSTODIAN

The Custodian has the same responsibilities as a Web Author, plus:
• Choosing and setting up other Custodians in their area of jurisdiction (e.g. department/branch).
• Choosing and setting up Web Authors.
• Making sure users that they set up have Internet access.
• Approving content.

It's very important that when a Custodian sets up another Custodian or Web Author, the new user is given these Content Management Guidelines, and its implications are discussed with them. A new user should not be set up on content management system before they have been sent for training (contact the Content Manager about this).

When approving an item of content, the Custodian is responsible for assessing if they're the best-qualified person to be approving that content.

They must also make sure that the content is:

• accurate
• up-to-date
• relevant
• complete
• prepared according to this policy.

Custodians should not change life events or topics, as they are used to build the generated navigation (i.e. links) on the portal. They have been pre-populated in order to cater for as wide a variety of information as possible in a standardised way. Should any Custodian wish to add a life event or topic, they should create the item in Bee and send it for authorisation to the Content Manager.

Each Head of Department shall be a custodian of the page relevant to their line function.

16.5 CONTENT MANAGERS RESPONSIBILITY

The Content Manager's role is to give overall direction and support for the portal for instance in choosing Web Authors and Custodians, and in strategising the nature of the content to appear on the website. This role shall be assigned to the incumbent responsible for communication in the Municipality.

The Content Manager's role is to give direction and support.
In the area of direction, to:

• Create and update the Municipal website Content Management Guidelines.
• Monitor implementation of the Guidelines.
• Strategise the content to go onto the portal, including language variants.
• Point departments to gaps in their online content.
• Do quality control of content.
• Ensure accountability for content approved.

In the area of support, to:
• Help departments decide what to put online.
• Train users about their roles and responsibilities, how to write for the Web, and how to use
the content management system.
• Help users understand the implications of these content management guidelines.

16.6 PRINCIPAL CUSTODIANS RESPONSIBILITIES

The Municipal manager is the Chief information Officer of the Municipality; he/she shall be ultimately responsible for all the content on the website.

16.7 WEB CONTENT MANAGEMENT LOGIN

When you're issued a username and password for web content management, they're yours and yours only. Do not 'lend' them to other users to update or approve content. If someone needs to work on content on Bee, then a Custodian must issue them with a username and password – even if they're not a regular user.

16.8 WHAT PROMPTS CONTENT UPDATING?

There are three prompts for content being updated:

16.8.1 DEPARTMENT-INITIATED

Departments should be updating their information and creating new content on a regular basis.

16.8.2 CUSTOMER-INITIATED

Requests for information will be made by customers via the portal, the call centre and the Municipal offices.

16.8.3 CONTENT MANAGER-INITIATED

The Content Manager will be constantly assessing the content of the website and will request departments to update/create content**.**

16.9 WEB CONTENT POLICY

This content policy is intended to guide the preparation of content for publication on the website

16.9.1 ACCURACY

Information entered into the website must be accurate. You are writing on behalf of the Municipality– the material you enter on the website is presenting the Municipality whole world.

An important aspect of accuracy is that the content must be **up to date**. If for instance there is an old version of information or documents on the site, there could be legal ramifications for the Municipality.

Remember that when you put information on the portal, it is as 'official' as if it was printed at the Government Printer or anywhere else.

16.9.2 POLITICS

The Municipality is apolitical and party political interests should not be represented on the site.

16.9.3 RELIGION

The Municipal website seeks to provide information to a wide range of people. Content should be written so as not to alienate people of any religion. Where religious terminology or references are used, make them inclusive of all religions, as opposed to exclusive. Policy cross-reference: South Africa's National Constitution clause on freedom of religion, belief and opinion clauses 15.1 (1) and (2)

16.9.4 REFERRING TO RACE

Where it's necessary to refer to race, the portal will use the same words as Statistics South Africa:

- black African
- white
- coloured
- Indian

Note that African and Indian are capitalised as they are derived from proper nouns.

When referring to everyone that's not white, use 'black'.

Use these words as adjectives, not nouns:

- blacks in the district
- black people in the district

16.9.5 REFERRING TO DISABILITY

Referring to disability is a difficult area, and there are a number of approaches. Here's a summary of the main points:

Avoid terms that group people as if they were identical, such as "the blind" and "the deaf". Try to use the word 'person' along with an adjective:

- the disabled
- disabled people/students

16.10 DEVELOPING AND MANTAINING THE WEBSITE

The Municipality has the responsibility to make Municipal information and services available easily, widely and equitably. Websites are one of the initiatives that can be used by the Municipality for the electronic dissemination of information.

The website shall be comprehensive online depositories for municipal information, while the municipality must be responsive to the needs of the citizens by providing as many as possible services online. The website shall also provide a medium for two-way communication between municipality and citizens.

While it is important for website to reflect the character of the municipality, users of municipal websites shall also benefit from a standardised approach. There is a need for some level of consistency and conformity between the municipality's website to assist the user to find information easily.

16.10.1 DESIGNING THE WEBSITE

The website's content shall be relevant to its aim, purpose and audience. It shall be broad enough and deep enough to meet the audience's needs.

The website shall contain the following:

ABOUT US

This category shall provide an overview or introduction to the municipality and shall include the following information:

- Profile, contact details and responsibilities of the Mayor, Deputy Mayor, Speaker, Chief Whip, EXCO members and Councillors.
- Council structure and the terms of reference of the various committees within the Municipality.
- Vision, Mission, Goals, Objectives and strategies of the Municipality.
- Organisational structure and the responsibilities of units.
- Municipal administration showing the Municipal Manager and the Heads of Department outlining their performance contracts, responsibilities and a brief profile.
- Vacancies with the application form and recruitment policy and procedure, there must also be a link to the Municipality's human resource policies.
- Historic background of the Municpality

CONTACT US

This menu shall have the complete contact information for the municipality covering the following contact information being telephone numbers, fax numbers, email addresses, postal address and the physical address.

The page shall also have an e-form which will allow users to email from the site.

SERVICES

Services rendered by the municipality to the public, investors, business and organisations, foreign nationals and other government departments.

PROGRAMMES

The various programmes, projects and campaigns run by the Municipality or by other government departments in the municipality.

ACCESS TO INFORMATION

All the documents which are listed in section 16 of this policy and other documents required on the website. This shall also include speeches, newsletters, legislations, strategic documents, publications and media statements.

RESIDENTS
All information required or intended for residents of the municipality, this shall include amongst others rates and tariffs, notifications, resident facilities available, frequently asked questions etc.

VISITORS
This section of the website shall be dedicated to tourists visiting the municipality or those wishing to visit the Municipality. the Menu shall cater for places to stay, things to do, areas of interest, food and drink and activities within the municipality not excluding historic background and heroes.

BUSINESS
The business section of the website shall be intended for all those wishing to do business with the municipality or those whose businesses are based in the municipality. This section shall have the following sub sections, tenders, quotations, business incentives supplier database registration, expression of interest and business information. Businesses will also be able to advertise on the municipal business directory at a cost.

INVESTMENT
Investment shall be dedicated to those investors wishing to fund the municipality or those wishing to invest in the municipality, this portion shall be dedicated to the Local Economic Development unit

FRONT PAGE
The front page of the website shall be attractive and will be designed in line with the municipal corporate manual. The following information shall be depicted on the front page:

- Picture of the Mayor on the right hand side of the page with his/her contact details, clicking on the picture shall lead user to the Mayors blog.
- Calendar of meetings which shall be updated weekly, the calendar shall be populated with all the meetings and official municipal events which will be taking place in that month.
- Latest news events or the latest information update.
- Links banner which takes you to a page with all the relevant government and organisation links.
- FAQ banner which takes you to the frequently asked questions page
- IDP, Reports and Budget banners
- “About the website”. This should include an orientation to the website, for example the purpose and aim of the website, the intended target audiences, an overview of the scope of information on the website and site-specific help information.
- “Terms and conditions of use”. This page must contain provisions with regard to issues such as copyright, intellectual property rights and security. It must also include a disclaimer to protect the owner department from any liability.
- “Feedback”. The website shall have a facility that provides a means for users to give feedback or comments about the website.
- Site map an area where new information posted on the website is announced. This can be the home page or a page specifically created for this purpose.

- Search functionality

17 USER DECLARATION OF INDEMNITY

I _____ (Full Name and Surname) hereby declare that I am employed by the 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

Policy Approval

This Policy was approved at a full Council Meeting held on _____day of _____ (Month) _____ (Year) at UMngeni Municipality.

_____	_____	_____
Name and Surname	Designation	Signature
_____	_____	_____
Name and Surname	Designation	Signature
_____	_____	_____
Name and Surname	Designation	Signature
_____	_____	_____
Name and Surname	Designation	Signature
_____	_____	_____
Name and Surname	Designation	Signature