ICT USER POLICY

FOR

MSINGA LOCAL MUNICIPALITY

MSINGA MUNICIPALITY

TABLE OF CONTENTS

CONTENTS

1. PREAMBLE

1.1 Electronic communication is an indispensable business tool within the Msinga Municipality.

1.2 Despite its benefits, unrestrained and uncontrolled electronic usage can cause a serious business liability.

1.3 It is reckoned that users of the Municipality's electronic communication system can intentionally or unintentionally infringe copyrights, violate trade secrets and trade marks, defame other people and businesses/institutions, harass individual/s, and commit the Municipality to contracts.

1.4 This can cause damage to the municipality, as it is generally liable for the acts of the users.

1.5 In order to protect both the Municipality and the users' interests, it is important that employees are made aware of the limitations placed on their access to the Municipality's electronic communication systems.

2. PURPOSE OF THE POLICY

2.1 To usher in proper and sound management of the network and security systems.

2.2 To set responsibilities and limitations of the PC users.

2.3 To foster discipline with regards to the Municipality's confidential database.

2.4 To give effect to the general protection of the Municipality's interests in respect of use of the electronic communication systems.

3. APPLICATION OF THE POLICY

This policy shall also apply to all Municipal Councilors and employees for the period of their tenure as full-time Councilors.

4. DEFINITIONS

4.1 **Associate:** A person or an organization having partial rights or subordinate status whilst doing business with or for the Municipality.

4.2 **Browse:** Read computer data files.

4.3 **Computer:** An electronic device that processes data according to a set of instructions.

4.4 **Copyright:** An exclusive legal right, given to the originator or his/her assignee for a fixed number of years.

4.5 **Hardware:** The mechanical and electronic components of a computer.

4.6 **EXM:** For the purpose of this policy, the meaning of the EXECUTIVE MANAGER shall include the Municipal Manager, Senior Managers and Managers.

4.7 **Megs (Megabytes):** A measure of data capacity.

4.8 **Network:** A chain of interconnected computers.

4.9 **Software:** The programs and other operating information used by a computer.

4.10 **Users:** Any authorized person who is given an access to a Computer Set (PC) of the Municipality, including any person to whom the Computer set is allocated to for the purpose of executing official duties.

4.11 **Web:** Complete network of inter-connected series.

4.12 **Chain letter:** One of a sequence of letters in electronic form, each recipient in a sequence being requested to a specific number of other people.

4.13 3g Card: referred to the connection Mobile access.

4.14 VPN: Virtual private network.

5. NETWORK USERS' REGULATIONS

5.1 Financial Servers, Exchange & File Server

5.1.1 User Access

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

5.1.1.2 The EXECUTIVE MANAGER will allocate and determine the level of access to each user.

5.1.1.3 All account creation requests shall be done in writing by the EXECUTIVE MANAGER and forwarded to the System Administrator.

5.1.2 User Etiquette

5.1.2.1 Multiple logins per user will be allowed up to the maximum of 2 (because there is a legal limit on licenses).

5.2.1.5 **Managing Network Access Controls**

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

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

5.2.1.6 Controlling Access to Operating System Software

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

5.2.1.6.2 Notwithstanding, clause 5.2.1.7.1, access shall be operated under dual control requiring the specific approval of senior management.

5.2.1.7 Securing Against Unauthorized Physical Access

5.2.1.7.1 Physical access to the server room which shall be regarded as a high security area shall be controlled with strong identification and authentication techniques, at all times.

5.2.17.2 Staff with authorization to enter such areas shall be provided with information on the potential security risks involved.

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

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

5.2.1.9 Monitoring System Access and Use

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

5.2.1.10 Giving Access to Folder drives, Files and Documents

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

5.2.1.11 Controlling Remote User Access

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

5.2.1.12 Accessing Municipal Network Remotely

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

5.2.1.12.2 Authorised Users shall access the network through VPN.

5.2.1.13 Permitting Third Party Access

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

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

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

5.2.1.13.3 Third party access to the Municipal network may be permitted in respect of the ICT Managed services.

5.2.1.13.4 Third party access shall be through VPN, and through the firewall, hardware to hardware connection may be considered and authorized under exceptional cases.

5.2.2 Web Browsing

5.2.2.1 No users are allowed to display or knowingly access any material that is obscene, profane, sexually oriented, threatening, racially offensive, illegal or morally unacceptable.

5.2.2.2 Web browsing should be strictly work related and kept to a minimum, without creating unnecessary traffic on the Internet line.

5.2.3 E-mail

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

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

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

5.2.3.2.2 Soliciting e-mails or Internet for commercial ventures, religious, political and personal causes or outside organizations;

5.2.3.2.3 Using e-mail for gossip, including personal information about users or others;

5.2.3.2.4 Emotive responses to business correspondence or work situations;

5.2.3.2.5 Forwarding e-mails likely to embarrass the sender or recipient;

5.2.3.2.6 Using the network for private ventures and/or personal gain.

5.2.3.2.7 Any threatening or abusive e-mail received by users shall be brought to the attention of the EXECUTIVE MANAGER who will take the appropriate action which may include legal action.

5.2.3.2.8 Attachments to emails shall be kept to a minimum, as most mail servers do not allow attachments larger than 2.5 Megs.

5.2.3.2.9 Users shall delete their e-mails (Inbox, Sent Items, Deleted Items) on a regular basis to free up space on the server.

5.2.3.2.10 Users shall save and/archive their e-mails (Inbox and Sent Items) on a regular basis to free up space on the server.

5.2.3.2.11	The System Administrator/ICT personnel reserves the right to delete e-mails, if space becomes an issue, but users on leave/away shall be taken into consideration in this regard and the user in question shall first be informed before deletion takes place.
5.2.3.2.12	Private e-mail correspondence should be limited to a minimum, the quantum will be regulated.
5.2.3.2.13	Chain letters shall not be permitted.
5.2.3.2.14	E-mail sent by a user is the express property of the MLM but this excludes any e-mail where a copyright applies.
5.2.3.2.15	The MLM has the right, but not the duty, to monitor all e-mails to ensure compliance with this policy.
5.2.3.2.16	The following disclaimer will automatically be added to all out going e-mails that will protect the MLM from any legal action as far as e-mail abuse is concerned:

"The Msinga Municipality exercises no control over information contained in any e-mail message originating from within the organisation. The Municipality makes no representation relating to the completeness or accuracy and accepts no responsibility for any loss, damage or liability that is incurred by reliance on the content hereof by the recipient or any other party. Each page attached hereto must also be read in conjunction with any disclaimer, which forms part of it.
Confidentiality: The e-mail is privileged and confidential and for use of the addressee only. Should you have received this e-mail in error, please return it to fanozi.sithole@msinga.org. Dissemination, disclosure, copying or any similar actions of the content of this e-mail is strictly prohibited."

6. ACQUISITION OF NEW EQUIPMENT

6.1 Acquisition

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

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

6.1.3 New computer equipment shall be purchased and shall conform to the following minimum standard of quality and ability:

6.1.4 Hardware

6.1.4.1 Desktop

6.1.4.1.1 Intel Dual Core 2.00 Ghz chip
6.1.4.1.2 1 GB DDR2 667 Memory
6.1.4.1.3 Minimum 250 GB Hard-Drive
6.1.4.1.4 DVD/CD writer
6.1.4.1.5 Built in speakers
6.1.4.1.6 Standard keyboard and mouse
6.1.4.1.7 17" LCD Monitor
6.1.4.1.8 Windows 7 professional
6.1.4.1.9 Security Cable with a set of keys

6.1.4.2 Laptop

6.1.4.2.2 2 GB DDR2 667 MHZ 1 DIMM
6.1.4.2.3 100GB 4200 rpm
6.1.4.2.4 250 GB HDD
6.1.4.2.5 DVD+/-RW DL Super Multi fixed Bluetooth
6.1.4.2.6 Built in speakers
6.1.4.2.7 Intel 802.11 a/b/g mini PCI card
6.1.4.2.8 Integrated TPM Security Module
6.1.4.2.9 WXGA (15.4)
6.1.4.2.10 Intel Media Graphics Accelerator X3100 UMA 384 MB
6.1.4.2.11 Windows 7 Professional with
6.1.4.2.12 Carry case.
6.1.4.2.13 Security Cable with a set of keys

***6.1.4.2.14* Issuing Laptop / Portable Computers to Personnel**

6.1.4.2.12.1 Line management shall authorize the issue of portable Computers. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices.

6.1.4.2.12.2 The Municipality will support purchase of laptops for and Level 0 to 6 employees, if the nature their work requires laptops.

6.1.4.2.15Using Laptop/Portable Computers

6.1.4.2.13.1Persons who are issued with portable computers and who intend to travel for business purposes shall be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimize the risks.

6.1.4.2.13.2Laptop computers are to be issued to, and used only by, authorized employees and only for the purpose for which they are issued for.

6.1.4.2.13.3The information stored on the laptop shall be suitably protected at all times.

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

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

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

6.1.4.3 Printer /s

6.1.4.3.1 Office jet with a minimum of 4 Megs of RAM and print speed of 10 pages per minute.
6.1.4.3.2 Office printers may be considered and approved for individual users based on the nature of their job, by line management.
6.1.4.3.3 Network printers shall be centralised and be managed and/or controlled under the supervision of Corporate Services Department.
6.1.4.3.4 Information classified as Highly Confidential or Top Secret, may never be sent to a network printer without there being an authorized person to safeguard its confidentiality during and after printing.

6.1.4.4 3g cards for users designated by the Municipal Manager.

6.1.4.5 Installing New Hardware

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

6.1.5 **Installing and Maintaining Network Cabling**

6.1.5.1 Network cabling shall be installed and maintained by qualified Engineers to ensure the integrity of both the cabling and the wall mounted sockets. Any unused network wall sockets should be sealed-off and their status formally noted.

6.1.6 Controlling IT Consumables

6.1.6.1 IT Consumables must be purchased in accordance with the

Municipality's Supply Chain Management Policy with usage monitored to discourage improper use.

6.1.7 Using Removable Storage Media including Diskettes, USB Memory sticks and CDs

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

***6.1.8* Contracting or Using Outsourced Processing**

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

***6.1.9* Moving Hardware from One Location to Another**

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

6.1.10 Recording and Reporting Hardware Faults

6.1.10.1 All information system hardware faults are to be reported promptly and Recorded in a hardware fault register.

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

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

***6.2.2* Software**

6.2.2.1 Microsoft Office 2007 or higher

6.2.2.2 Anti-Virus software

6.2.2.3 Windows 7 Professional

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

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

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

7. LIMITATIONS AND RESPONSIBILITIES OF USERS

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

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

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

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

7.5 No user shall be allowed to attach any equipment to the network or computers without prior authorization by the EXECUTIVE MANAGER in consultation with the Systems Administrator.

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

7.7 Users shall not be allowed to flood the network intentionally.

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

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

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

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

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

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

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

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

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

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

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

7.18.1 The user must reboot their PC at least once a week during working hours.

7.18.2 All users shall have their official user files on the H: drive.

7.18.3 All users shall be responsible for frequent updates (windows, antivirus, etc.).

7.19 Access for one user to another user's PC can only be authorized by the EXECUTIVE MANAGER or the users superior and must be done in consultation with the System Administrator.

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

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

8. USERS' SECURITY POLICY

8.1 Login and Passwords

8.1.1 Users shall not be allowed to give out their login and password to ANYONE.

8.1.2 Users shall not be allowed to use any other user's login and password to obtain unauthorized access to network resources.

8.1.3 Financial and Payroll system users must not leave their systems unattended to; the user shall either log out of the program before leaving his office or lock the office.

8.1.4 Approved login procedures must be strictly observed and users leaving their screen unattended must firstly lock access to their workstation or log off.

8.1.5 Passwords:-

8.1.5.1 Users shall use secure passwords of no less than 6 and no more than 7 characters long.

8.1.5.2 Users shall use a combination of alphanumeric and special characters in order to produce the most secure passwords that cannot be easily guessed.

8.1.6 Users shall not write down or store their passwords in any physical form.

8.1.7 Users shall not misrepresent themselves or their data on the network.

8.1.8 Users shall not be allowed to monitor another user's data communication, nor read, copy, change or delete another user's files or software, without the owner's permission.

8.1.9 Users shall not be allowed to give any person remote access to their computer.

8.1.10 Users shall not circumvent data protection schemes or exploit security loopholes.

8.1.11 Users shall report any suspected breach of security to the System Administrator for investigation and verification.

8.1.12 User's password can be changed by the ICT personnel on authorization by the line management, due to operational reasons.

8.2 Network and Security Policy Violation

8.2.1 In the event of an incidence of violation of either the Network or Security Policy, the following shall apply:-

8.2.1.1 Accidental and unintentional violations shall not be classified as offences.

8.2.1.2 Acts of violations against this policy will be dealt with in terms of **ANNEXURE "A"** of this policy and the disciplinary procedure of the MLM.

8.2.1.3 Not withstanding the scope of application of and definition of an employee in this policy, this disciplinary code applies only to individuals who are defined as employees of MLM by law.

9. COMMENCEMENT

This Policy will come into effect on the date of adoption by Council.

10 INTERPRETATION OF THIS POLICY

10.1 All words contained in this policy shall have the ordinary meaning attached thereto, unless the definition or context indicates otherwise.

10.2 The dispute on interpretation of this policy shall be declared in writing by any party concerned.

10.3 The Office of the Municipal Manager shall give a final interpretation of this policy in case of written dispute.

10.4 If the party concerned is not satisfied with the interpretation, a dispute may then be pursued with the South African Local Government Bargaining Council.

11 PERMANENT/TEMPORARY WAIVER OR SUSPENSION OF THIS POLICY

11.1 This policy may be partly or wholly waived or suspended by the Municipal Council on temporary or permanent basis.

11.2 Notwithstanding clause No. 11.1 the Municipal Manager may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to Council.

12 COMPLIANCE AND ENFORCEMENT

12.1 Violation of or non-compliance with this policy will give a just cause for disciplinary steps to be taken.

12.2 It will be the responsibility of Council to enforce compliance with this policy.

13 AMENDMENT AND/OR ABOLITION OF THIS POLICY

This policy may be amended or repealed by Council as it may deem necessary.

INTERNET USAGE POLICY

Policy: Access to the Internet through the MSINGA MUNICIPALITY network is a privilege. Users granted this privilege must adhere to strict guidelines concerning the appropriate use of this information resource. Users who violate the provisions outlined in this document are subject to disciplinary action up to and including termination. In addition, any inappropriate use that involves a criminal offense will result in legal action. All users are required to acknowledge receipt and understanding of guidelines contained in this document.

Purpose: To define policies and procedures for access to the Internet through the MSINGA MUNICIPALITY network infrastructure.

Scope: This policy applies to all personnel with access to Internet and related services through the MSINGA MUNICIPALITY network infrastructure. Internet Related services include all services provided with the TCP/IP protocol, including but not limited to

Electronic Mail (e-mail), File Transfer Protocol (FTP), Gopher, and World Wide Web (WWW) access.

Procedure:

1.0 ACCEPTABLE USE

1.1. Access to the Internet is specifically limited to activities in direct support of official MSINGA MUNICIPALITY business.

1.2. In addition to access in support of specific work related duties, the MSINGA MUNICIPALITY Internet connection may be used for educational and research purposes.

1.3. If any user has a question of what constitutes acceptable use he/she should check with the IT Unit for additional guidance. Management or supervisory personnel shall consult with the Information Services Manager for clarification of these guidelines.

2.0 INAPPROPRIATE USE

2.1. The MSINGA MUNICIPALITY, Internet access shall not be used for any illegal or unlawful purposes. Examples of this would be the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials

2.2. Use of MSINGA MUNICIPALITY electronic mail or messaging services shall be used for the conduct of MSINGA MUNICIPALITY, business only. These services shall not be used to harass, intimidate or otherwise annoy another person.

2.3. The MSINGA MUNICIPALITY, Internet access shall not be used for private, recreational or other non-MSINGA MUNICIPALITY related activity.

2.4. The MSINGA MUNICIPALITY Internet connection shall not be used for commercial or political purposes.

2.5. Use of the MSINGA MUNICIPALITY, Internet access shall not be used for personal gain such as selling access of a MSINGA MUNICIPALITY user login. Internet access shall not be used for or by performing work for profit with MSINGA MUNICIPALITY resources in a manner not authorized by The MSINGA MUNICIPALITY.

2.6. Users shall not attempt to circumvent or subvert security measures on the MSINGA MUNICIPALITY's network resources or any other system connected to or accessible through the Internet.

2.7. MSINGA MUNICIPALITY users shall not use Internet access for interception of network traffic for any purpose unless engaged in authorized network administration.

2.8. MSINGA MUNICIPALITY users shall not make or use illegal copies of copyrighted material, store such copies on MSINGA MUNICIPALITY equipment, or transmit these copies over the MSINGA MUNICIPALITY network.

3.0 INTERNET AND E-MAIL ETIQUETTE

3.1. MSINGA MUNICIPALITY employees shall ensure all communication through MSINGA MUNICIPALITY e-mail or messaging services is conducted in a professional manner. The use vulgar or obscene language is prohibited.

3.2. MSINGA MUNICIPALITY users shall not reveal private or personal information without specific approval from management.

3.3. Users should ensure that e-mail messages are sent to only those users with a specific need to know. The transmission of e-mail to large groups or messages with large file attachments should be avoided.

3.4. Electronic Mail is not guaranteed to be private. Messages transmitted through the MSINGA MUNICIPALITY e-mail system or network infrastructure are the property of MSINGA MUNICIPALITY and are therefore subject to inspection.

4.0 SECURITY

4.1. MSINGA MUNICIPALITY users who identify or perceive an actual or suspected security problem shall immediately contact the MSINGA MUNICIPALITY Information Systems Security Manager.

4.2. Users shall not reveal account password or allow another person to use their account. Similarly, users shall not use the account of another user.

4.3. Access to MSINGA MUNICIPALITY network resources shall be revoked for any user identified as a security risk or a demonstrated history of security problems

5.0 PENALTIES

5.1. Any user violating these policies is subject to the loss of network privileges and any other MSINGA MUNICIPALITY disciplinary actions deemed appropriate.

6.0 USER COMPLIANCE

6.1. All terms and conditions as stated in this document are applicable to all users of the network and the Internet connection.

6.2. All users must agree to abide by this policy by signing the Acknowledgement of Receipt and Understanding form

ANNEXURE "A"

NETWORK AND SECURITY POLICY

DISCIPLINARY CODE APPLICBLE TO MUNIICPAL OFFICIALS

Nature Of Misconduct	*First Offence*	*Second Offence*	*Third Offence*
1. Causing Disruptions in conflict with 7.1 & 7.7.	Written Warning	Final Written Warning	Dismissal
2. Disclosure: unauthorized information; either personal or confidential	Final Written Warning	Dismissal	
3. Illegal activities in terms of 7.5, 7.8, 7.9, 7.12 and 7.19.	Final Written Warning	Dismissal	
4. Illegal attachments and installations on PC's in terms of 7.4 and 7.13.	Dismissal		
5. Leaving Financial and Payroll System on PC unattended to in terms of 8.1.3.	Final Written Warning	Dismissal	
6. Misrepresentation in terms of 8.1.5.	Final Written Warning	Dismissal	
7. Electronic vandalism in terms of 7.11.	Dismissal		

NB: In the event of any disciplinary action being taken against any Network user, clause 3 and 6 of the Municipal's Disciplinary and Grievance procedure shall apply at all times.

DISCIPLINARY CODE APPLICBLE TO MUNIICPAL COUNCILLORS

Nature Of Misconduct	*First Offence*	*Second Offence*	*Third Offence*
1. Causing Disruptions in conflict with 7.1 & 7.7.	Written Warning	Final Written Warning	Disconnection from the networkl
2. Disclosure: unauthorized information; either	Matter reported to the Council.	Disconnection from the network	

personal or confidential			
3. Illegal activities in terms of 7.5, 7.8, 7.9, 7.12 and 7.19.	Matter reported to the Council.	Disconnection from the network	
4. Illegal attachments and installations on PC's in terms of 7.4 and 7.13.	Disconnection from the network		
6. Misrepresentation in terms of 8.1.5.	Matter reported to the Council.	Disconnection from the network	
7. Electronic vandalism in terms of 7.11.	Disconnection from the network		

Mr. TL Kunene (Speaker)

Mr. SL Sokhela (Accounting Officer)

Resolution No: _____

Review Version No: 2019

THE MUNICIPAL MANAGER
2019 -05- 29
MSINGA MUNICIPALITY
PRIVATE BAG X 530
TUGELA FERRY - 3010