MSINGA MUNICIPALITY

I.C.T Policy
2020-2021

1. INTRODUCTION

The IT Department has been mandated to be the main custodian of the IT Systems Hardware and Software in the Municipality. It is charged with ensuring that the IT hardware and software, data, servers, firewalls and business applications are all functioning to optimal levels of efficiency, that the networking and telecommunications are available to users at all times.

1.1 PURPOSE

This Disaster Recovery Plan document is aimed at the IT Disaster Recovery Program for recovering IT systems operations after a disaster. The plan describes the preparation and actions required to effectively respond to a disaster, assign responsibilities and describe procedures for testing and maintaining the plan.

1.2 OBJECTIVES

The primary objective of Disaster Recovery Plan is to protect the organisation in the event that all or part of its operations or computer services is rendered unusable. Preparedness is the key.

The planning process should minimise the disruption of operations and ensure some level of organisational stability and an orderly recovery after a disaster.

Other objectives of the Disaster Recovery Plan included:

- Providing a sense of security
- Minimize risk of delays
- Guaranteeing the reliability of standby systems
- Providing a standard for testing the plan
- Minimise decision-making during a disaster

1.3 SCOPE

This Disaster Recovery Plan is focused only on the municipal-owned and managed IT systems.

This plan addresses all preparation and steps necessary to restore processing or those systems so that the participating applications can continue processing after a disaster has rendered any or all the systems inoperable.

1.4 DISASTER RECOVERY STRATEGY

Should the IT systems encounter a disaster that prevents them from functioning, the IT Department and IT service providers should be prepared to provide adequate computational, data storage and data communications services and facilities on cloud disaster recovery resource for the participating applications.

The cloud disaster recovery resource is a fully operational storage facility that is prepared to host the user data. Payday (Payroll System) and Munsoft are backed up monthly by the service provider and backup and restore certificates are sent to the municipality as proof of backup.

4. ROLE OF THE INFORMATION TECHNOLOGY (IT) MANAGER

4.1 No new computers, printers, and/or any computer equipment shall be bought without approval and authorisation from the IT Manager.

4.2 No software package is to be purchased and loaded without the approval and authorisation from the IT Manager.

4.3 The IT Manager MUST ALWAYS be advised of >

4.3.1 All computer faults before anyone or any service provider from outside is called to fix the problem.

4.3.2 Any computer equipment which is being moved from one location to another.

5. ACCEPTABLE USE POLICY - DESKTOPS AND LAPTOPS

This policy defines end-user acceptable use of municipal IT equipment. The policy applies to desktops, laptops, printers, and other equipment provided by the Municipality. Anyone that uses municipal equipment including employees, vendors, contractors, and visitors, must adhere to this policy. Acceptable use applies to proper care, handling and maintenance of equipment as well as following documented security policies relating to equipment use.

5.1 User Responsibilities

Users shall use municipal - provided IT equipment responsibly and for municipal business purposes only. Appropriate use policies are:

5.1.1 Active desktops and laptops may not be left unattended for prolonged periods of time. Users should secure their workstation when leaving the workstation unattended.

5.1.2 Municipal information displayed on screens or on reports shall be treated as confidential and private. Users must guard municipal information from unauthorized access or use. Any employee-signed confidentiality agreement shall fully apply to information accessed with municipal IT equipment.

5.1.3 Managers are responsible to ensure that their employees are adequately trained on appropriate use of IT equipment and that they adhere to this policy.

5.1.4 Users may not grant access to non-employees, including vendors or contractors, without approval of their manager or approval by the IT Department.

5.1.5 Users shall keep their equipment clean and free from dust. Users shall maintain "breathing space" around equipment in accordance with equipment installation instructions.

5.1.6 Users shall not eat or drink at their workstation.

5.1.7 Desktop acceptable use policies apply equally to portable devices, including laptops, notebooks and cell phones.

5.1.8 All acceptable use polices apply equally to non-municipal provided equipment if the equipment accesses municipal Information or municipal networks.

5.1.9 Users who access municipal information and computer systems from remote locations must adhere to this policy.

5.1.10 Municipal-provided equipment shall be kept in a secure manner so that the employee's household members and others do not have access to the device when not in the office.

5.1.11 Users should not store municipal information or files locally only. The use of shared or network drives for all municipal information is required.

5.1.12 Users are responsible for backing up files stored on their desktop or laptop. The Municipality does not provide backups at the desktop level.

5.2 Prohibited practices

Any activity, action, or lack of action on the part of a user that damages the municipality or compromises security or confidentiality is prohibited. Examples of prohibited practices include:-

5.2.1 Installing new desktops or equipment without prior approval by the IT Department.

5.2.2 Upgrading equipment or adding peripheral equipment without prior approval of the IT Department.

5.2.3 Downloading and/or installing programs that are not specifically approved by the IT Department.

5.2.4 Using unlicensed software. Users may not copy and share software that is installed on their desktops or laptops with other users.

5.2.5 Using programs or Internet web sites that compromise the privacy of customers or employees.

5.2.6 Removing or compromising desktop virus protection programs.

5.2.7 Opening email attachments that are inappropriate or from someone you do not know.

5.2.8 Using municipal-provided IT equipment for non-business reasons or for personal gain.

5.2.9 Unauthorized attempts to break into any workstation.

5.2.10 Unauthorized access to municipal files, programs, databases, or confidential information.

5.2.11 Sending or posting confidential files to unauthorized persons.

5.2.12 Failing to fully cooperate with IT security investigations.

5.2.13 Allowing co-workers or other users to use your desktop without approval of your manager or by the IT Department.

5.2.14 Sharing password information or displaying it in plain view on or around your desktop. Users must secure their passwords and not reveal them to others.

6. ACCEPTABLE USE POLICY - EMAIL

This policy defines end-user acceptable use of municipal-provided email services. This policy applies equally to on-site usage as well as remote usage of municipal email.

When using municipal email, users shall follow these guidelines :-

6.1 User Responsibilities

6.1.1 E-mail users shall use e-mail in accordance with general communications policies of the Municipality.

6.1.2 Municipal - provided e-mail generally shall be used for business communications only. Users may use municipal e-mail for personal communication as authorized by their department manager.

6.1.3 Users understand and agree that they shall not have a right to privacy when using municipal e-mail or municipal assets for electronic communications, even if those communications are of a personal nature.

6.1.4 Departmental heads and/or the Human Resources Department should immediately advise the IT Department of any resignations so that their

e-mail and business application access credentials are disabled (terminated) for security reasons.

6.2 Prohibited Practices

6.2.1 Users should not open e-mails or e-mail attachments from persons unknown to them. Opening of unknown or suspicious attachments can have serious consequences for the Municipality in terms of viruses or computer worms. Users should contact the IT Department if there is even a slight concern about an e-mail attachment.

6.2.2 Users should not respond to spam e-mails or unsolicited
advertisements. Responding will multiply the amount of spam received. Unsolicited e-mails should be deleted or reported to the IT Department.

6.2.3 Users may not use e-mail to solicit employees for any purpose, including charitable purposes, without the written approval of their department manager.

6.2.4 Users may not forward or promote spam or joke e-mails, and
particularly may not send spam or joke e-mails to group e-mail addresses.

6.2.5 Users should not access, create, display, download, save or transmit threatening, racist, sexist, obscene, offensive, annoying or harassing language and/or materials such as broadcasting unsolicited messages or sending unwanted mail.

6.2.6 Users may not use e-mail for purposes that violate legal or Municipality policies regarding gambling, hate, pornography, or other inappropriate purposes.

7. ACCEPTABLE USE POLICY - INTERNET

This policy defines end-user acceptable use of municipal-provided Internet access. This policy applies equally to non-municipal provided Internet access made while on municipality premises.

When using Internet, users shall follow these guidelines:-7.1

User Responsibilities

7.1.1 Municipal-provided Internet access generally shall be used for business purposes only. Users may use Internet for personal reasons

as authorized by their municipal department manager.

7.1.2 The IT Department shall be responsible for installing and updating anti-virus software on all computers. Users will be responsible for weekly or monthly desktop scanning which is normally required to eradicate spyware and latent viruses.

7.1.3 Users understand and agree that they shall not have a right to privacy when using Internet on municipal-provided equipment.

7.1.4 Users understand and agree that the Municipality may severely limit access, including the use of controls that prevent access to sites deemed inappropriate by the Municipality. The Municipality has the right to monitor and control Internet usage at its sole discretion.

7.1.5 Users agree that the Municipality will decide which websites can be accessed using the guidelines provided by the service provider. This will be monitored on an ongoing basis and amended from time to time as required.

7.1.6 Website can automatically be blocked by the service provider if the site is exposed from a security perspective or if the site is used for inappropriate purposes.

7.2 Prohibited Practices

When using Internet, users must follow these guidelines:-

7.2.1 Users should not download software or images unless they are from a trusted source, and then only if authorized by the IT Department. Opening of unknown or suspicious programs or images can have serious consequences for the Municipality in terms of viruses or computer worms. Users should contact the IT Department before they download any files from the Internet.

7.2.2 Users should not provide their e-mail address when registering at a website unless the web site has a clear policy that they will protect e-mail privacy.

7.2.3 Users should not use the Internet for on-line radio or television access without permission from the IT department. Sites that provide
streaming content have a significant impact on network resources and impact network performance and responsiveness.

7.2.4 Users may not use Internet for purposes that violate legal or municipal policies regarding gambling, hate, pornography, or other inappropriate purposes.

7.2.5 Users shall not access, create, display, download, save or transmit any text, file picture, graphic or sound clip or engage in any conference that includes material which is obscene, libellous, indecent, vulgar, profane, and lewd or which advertises any product or service not permitted to minors by law.

7.2.6 Users shall not engage in activities that damage hardware or software, disrupt communication, waste systems resources, or overload networks with excessive data.

7.2.7 Users shall not access chat rooms to carry out non-business related matters.

8. ACCEPTABLE USE POLICY - BUSINESS APPLICATIONS

This policy defines end-user acceptable use of municipal business application software. This policy applies to all software identified by the municipality as a business application. General Accounting and Financial Management software, Electrical SCADA, CIS are examples of business applications. Anyone that uses municipal business applications including employees, vendors, contractors, and visitors, must adhere to this policy.

8.1 User Responsibilities

Users shall use municipal-provided application software responsibly and for municipal business purposes only. Appropriate use policies are:-

8.1.1 All IT Infrastructure Acceptable Use Policies fully apply to application software usage. This includes the requirement that active desktops and laptops may not be left unattended for prolonged periods of time. Users should secure their workstation when leaving the workstation unattended.(See Section 5)

8.1.2 Municipal information display on equipment or on reports shall be treated as confidential and private. Users must guard municipal information from unauthorized access or use. Any employee-signed confidentiality agreement shall fully apply to information accessed with municipal IT Equipment.

8.1.3 Managers are responsible to ensure that their employees are adequately trained/educated on appropriate use of municipal software applications and that they adhere to this policy.

8.1.4 Managers are responsible to assure that users have adequate access to applications, but do not have access that is inappropriate for their job function or otherwise represents an unnecessary security risk for the municipality.

8.1.5 Users may not grant access to non-employees, including vendors or contactors, without approval of their manager or approval by the IT Department.

8.1.6 Users who access municipal information and computer systems from remote locations must adhere to this policy.

8.1.7 Users should promptly report software problems or apparent defects to their manager. Managers should work with the municipal software primary contact to determine if the issue is software related, and if so, how best to have it fixed.

8.2 Prohibited Practices

Any activity, action, or lack of action on the part of a user that damages the municipality or compromises security or confidentiality is prohibited. Examples of prohibited practices include:-

8.2.1 Installing new software applications without prior approval by the IT Department. This includes downloading software from the Internet, even if there is no charge for the software. Downloading applications for evaluation purposes is also prohibited unless approved in advance by the IT Department.

8.2.2 Sharing passwords with other users. Users shall not post or display their passwords where they can be seen by others.

8.2.3 Attempting to access applications without approval. Employees shall not attempt to gain access or hack into an application that they are not authorized to access.

8.2.4 Using unlicensed software. Users may not copy and share software that is installed on their desktops or laptops with other users.

8.2.5 Using programs or Internet web sites that compromise the privacy of customers, patients, or employees.

8.2.6 Unauthorized access to municipal files, programs, databases, or
confidential information.

8.2.7 Sending or posting confidential files to unauthorized persons.

8.2.8 Failing to fully cooperate with IT security investigations.

9. COMPLIANCE

Management in conjunction with the IT administrators of the Municipality may deem it necessary to search any computer drive or file system for alleged violation of this policy. Violations will be noted and reported. The Municipality retains the right to randomly monitor and intercept all Employee communication, regardless of whether they are of a business or personal nature, including but not limited to e-mail and Internet usage. Whenever an IT administrator is on-site at a branch or any satellite location, he or should test at random, compliance levels at the individual desktop level.

The monitoring of communications on the municipal IT infrastructure is not a "witch-hunting" exercise. It is necessary for the support and maintenance of this valuable infrastructure.

Users should report inappropriate e-mails, usage, handling or any policy violations to the IT Department immediately.

Note: Any Employee who abuses the privilege of Municipality-facilitated access to IT will be subject to corrective action. Any action (on IT facilities, computer equipment, business applications, e-mail or the Internet) that may expose the Municipality to risks of unauthorized access to data, disclosure of information, illegal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution. If necessary, the Municipality also reserves the right to advise appropriate legal officials of any illegal violations. Employees that

violate this policy will be disciplined and may be dismissed/terminated for serious or multiple violations.

10. COMMUNICATING THE IT POLICY

10.1 Copies of the IT policy shall be provided to all Heads of Department s who will then review the policy with all employees in their respective departments.

10.2 A copy of the IT Policy shall be sent via e-mail to each current employee of the Municipality, and shall include as final, a form for acceptance to the terms of this policy.

10.3 Each employee of the Municipality shall sign and date the acceptance form, and shall return the form to the Human Resources Department for retention in employee records.

10.4 The final draft of this policy shall be included within the company's "handbook" of company's policies, and shall be presented to all newly hired employees at the start of their employment.

10.5 Acceptance of the IT Policy by a new employee shall be denoted by signing and dating the acceptance form and returning the form to the Human Resources department for retention in employee records.

10.6 The municipal employee, who contracts for services provided by software contractors, or vendors/suppliers providing services to the Municipality, is responsible for providing the contractor/vendor/supplier with a copy of these policies before any access to Company IT/ facilities/assets is granted.

11. AMENDING THE IT POLICY

11.1 The Municipality reserves the right to amend these policies and practices at any time without prior notice and to take such further actions as may be necessary or appropriate to ensure compliance.

11.2 The Municipality's IT Policy shall be reviewed annually to comply with applicable state, local government laws, regulations and policies that govern the workplace.

11.3 Amendments to the IT Policy shall be reviewed and approved by Computer Steering Committee as designated by the SED: Corporate Services.

11.4 The amended draft of the policy shall be legally reviewed and approved before the amended policy is considered to be municipal policy.

11.5 The Municipality shall publish the amended IT Usage Policy in the workplace to ensure that all employees are notified of the amendments to the policy.

11.6 Copies of the newly amended policy shall be given to all Heads of Departments of the Municipality who will then review the policy with all employees from their respective departments.

11.7 Sign-off of the pre-existing IT Policy by a current employee of the Municipality shall constitute acceptance of the newly modified version.

11.8 All personnel employed by the Municipality subsequent to the IT Policy amendment(s), shall be required to sign the acceptance sheet to the terms of this newly amended municipal policy.

11.9 The municipal employee who contracts for services provided by software contractors, or vendors/suppliers providing services to the Municipality is responsible for providing the contractor/vendor/supplier with a copy of the amended policies before any further access to IT assets is granted.

Mr. TL Kunene
(Speaker)

Mr. SL Sokhela
(Accounting Officer)

Resolution No: _ 23/2020 SFC _