Logo

Information Communication Security Policies

Date Approved	Version	Resolution Number
22 February 2012	1	10.3.2
26 June 2015	2	11.7.2.2
30 June 2016	3	10.3.3
28 July 2017	4	020/OCM/17

The Information Technology Manager

Senqu Local Municipality

19 Murray Street

Lady Grey

Telephone (051) 603 1300

Facsimile (051) 603 0445

Website: www.senqu.gov.za

Table of Contents

Council Resolution

Council Resolution on ICT Risks in Senqu Municipality

The Council realises the strategic role that Senqu Municipality's ICT infrastructure plays in support and implementing Senqu Municipality's business processes. The Council also understands the potential impact that unavailability of Senqu Municipality's ICT infrastructure, or part of the infrastructure, can have on Senqu Municipality's ability to meet the needs of stakeholders and to deliver services to the community.

The Council therefore mandates the existence of the necessary environment to ensure the protection of Senqu Municipality's ICT infrastructure, services and support in the event of disruptions of any sort.

The Council provides its full support and commitment to the enforcement and governance of all aspects required to establish and maintain an ICT

Introduction

Information and information systems are critical and vitally important to the municipality. Without reliable information the municipality could be adversely affected, both financially and reputation wise. Therefore, this policy states the minimum requirements and the responsibility that all councilors, employees, temporaries, contractors and management must comply with in order to secure the municipality's information.

The Information Security Policies set out the approach taken to manage information security to ensure that information resources are properly protected against a variety of threats such as error, fraud, embezzlement, sabotage, terrorism, extortion, privacy violation, service interruption, theft and natural disaster, whether internal or external, deliberate or accidental.

SENQU Municipality management has a duty to preserve, improve, and account for all information and information systems. They must additionally make sure that information assets are protected in a manner that is at least as secure as other organisations in the same industry handling the same type of information. To achieve this objective, annual reviews of the risks to SENQU Municipality's information assets will be conducted. Similarly, whenever a security incident or audit finding indicates that the security of information or information systems is insufficient, management must promptly take remedial action to reduce the municipality's exposure.

The municipality's information must be protected in a manner appropriate to its sensitivity, value, and criticality. Security measures are therefore used regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. This protection includes restricting access to information based on the need-to-know principle.

Decision-making within the municipality is also critically dependent on information, as management need to be able to rely on the integrity of information in terms of accuracy, timeliness, relevance, completeness, confidentiality, criticality, etc. The awareness of and fine-tuning of such information is an important information management activity.

Information security requires the participation and support from all staff (including consultants, contractors, and temporaries) that will be provided with sufficient training and supporting procedures / policies to allow them to properly protect and manage the municipality's information assets.

It is the responsibility of all municipal staff to report any software malfunctions, security incidents, suspected viruses, faults, weaknesses or threats observed or suspected to systems or services to the Information Services, Information Security Officer or manager responsible for information/system security as soon as possible to enable the volumes and costs of incidents and malfunctions to be quantified and monitored.

Section 4 **ICT Security Policies**

Introduction

Executive Summary

The following policy statements constitute the core of the municipality's Information Security Policy for information and will be supported by specific information security directives, standards and guidelines as needed from time to time.

Classification - Information must be categorised into levels of sensitivity and protected in accordance with appropriate requirements as part of the risk management process. The sensitivity classification standard must be used throughout the municipality to ensure that the level of protection is commensurate with the controls required (security mechanisms) to protect the information against disclosure (confidentiality), modification (integrity) and / or destruction (availability and use).

Confidentiality - The confidentiality of all data, depending on classification and information security directives, will be protected before transmission over networks, and where indicated during the storage of such data.

Unless authorised by management, information may not be made available or disclosed to unauthorised individuals, entities or processes.

Measures should be implemented to protect information against unauthorised access, disclosure, copying, sniffing, eavesdropping and /or theft of information assets.

Availability - The continued availability and usability of services in accordance with business requirements must be ensured by implementing appropriate measures to prevent and recover from the loss of data due to acts of persons, system failures or disasters.

All information assets should be protected against:

- Theft, abuse or misuse
- Destruction, damage or contamination
- Denial of authorised / legitimate access
- Delay of use or access
- Natural disasters
- Computer virus infections

Integrity - The integrity of all data, depending on classification and information security directives, will be protected at all times before transmission over networks, and where indicated, also during the storage of such data.

All information assets should be protected against threats to data integrity including unauthorised modification, destruction, and misrepresentation of data and / or computer virus infections.

Non-Repudiation - All access to the municipality's technology resources is subject to positive identification and authentication of the user before access is granted.

Measures must be implemented to ensure the non-repudiation of all

financial transactions in accordance with official legislation and regulations. Processes must be implemented to allow for the non-repudiation of origin regarding sensitive e-mail.

Accountability - Measures must be implemented to ensure that it is possible to determine who is responsible for an action, when and from where. The measures must be in accordance with the security requirements as determined by the departmental manager.

Access Control - All data and information will be protected and safeguarded against unauthorised access. Access to technology resources will only be granted in line with the user's specific responsibilities (need-to-have principle).

Authentication - Measures must be implemented to uniquely identify or verify IT users, peripherals and / or programs and to assure individual accountability. The authentication mechanisms must be in accordance with the classification of the information that requires protection and may for example take the form of passwords, tokens, or biometric identification devices.

All users will access SENQU Municipality's information systems through at least the use of a unique user identification number and secret password. As a first line of defence, users should not select passwords that are easily guessable nor should personal passwords be shared with any other user.

Reporting of Security Incidents - All known vulnerabilities – in addition to all suspected or known violations – must be reported in an expeditious and confidential manner to the Office of the Information Security Officer or manager responsible for security. Unauthorised disclosure of the municipality's information must additionally be reported to the involved information owners. Reporting security violations, problems or vulnerabilities to any party outside the municipality without prior written approval of the Office of the Information Security Officer is strictly prohibited.

Any attempt to interfere with, prevent, obstruct, or dissuade an employee in their efforts to report a suspected information security problem or violations is strictly prohibited and cause for disciplinary action.

Exceptions - Exclusions based on a valid business need could be motivated for and formally authorised, in which case record would be kept of the exclusions to facilitate effective management / control processes.

Disciplinary Code of Practice

Violation of or failure to adhere to this policy or any of the supporting policies will be considered as misconduct and may result in disciplinary action.

Change Management

Introduction

The Information Resources infrastructure at the Municipality is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management process is essential.

From time to time each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

Audience

The Municipality Change Management Policy applies to all individuals that install, operate or maintain Information Resources.

Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Definitions, continued

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. The custodian is normally a provider of services. (Currently the IT Administrator is the Custodian)

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

Change:

- any implementation of new functionality
- any interruption of service
- any repair of existing functionality
- any removal of existing functionality

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of security vulnerability.

Emergency Change: When an unauthorised immediate response to imminent critical system failure is needed to prevent widespread service disruption.

Change Management

Change Management Policy

- Every change to the Municipality's Information Resources resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.
- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process.
- The ICT Steering Committee, appointed by the Council, will review change requests and to ensure that change reviews and communications are being satisfactorily performed.
- Minor changes may be approved by the person in charge of the ICT Section. These changes must be recorded and reported to the next meeting of the ICT Steering Committee. These changes include the installation, removal and replacement of equipment such as workstations, printers, scanners, batteries, inverters, UPSs, antennas, Wi-Fi devices, network cables, air conditioners and any hardware or software that does not affect the functioning of the servers or the network.
- All scheduled change requests must be submitted in accordance with change management procedures so that the ICT Steering Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- Each scheduled change request must receive formal ICT Steering Committee approval before proceeding with the change.
- The appointed leader of the ICT Steering Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
- Users must be notified of each scheduled or unscheduled change in accordance with the Change Management Procedures.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
  - Date of submission and date of change;
  - Owner and custodian contact information;
  - Nature of the change; and
  - Indication of success or failure.
- All the Municipality information systems must comply with an Information Resources change management process that meets the standards outlined above.

Disciplinary Actions	Violation of this policy may result in disciplinary action.
Supporting Information	1.1.1.1 This Security Policy is supported by the following Security Policy Standards.
Reference #	**1.1.2 Policy Standard detail**
12	The IR network is owned and controlled by IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
14	The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorised access to the data.
15	All changes or modifications to IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.

Patch Management

Introduction	Senqu Local Municipality is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. The Municipality has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.
Purpose	This document describes the requirements for maintaining up-to-date operating system security patches on all Senqu Local Municipality owned and managed workstations and servers.
Audience	The Municipality Patch Management Policy applies to workstations or servers owned or managed by the Municipality. This includes systems that contain organisation or customer data owned or managed by the Municipality regardless of location. The following systems have been categorized according to management: Microsoft Windows servers as well as Workstations (desktops and laptops) are managed by the Senqu Municipality IT Team with support from the External IT Support.
Definitions	**External IT Support**: A knowledgeable person from an external company that has a Network Maintenance and Support Contract with Senqu Municipality. **IT Team:** All staff that fall under the ICT Section of Senqu Municipality as defined by the Organogram. **Patch:** A piece of software designed to fix problems with or update a computer program or its supporting data. **Trojan:** A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions. **Virus:** A computer program that can copy itself and infect a computer without the permission or knowledge of the owner. **Worm:** A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth. **WSUS:** Windows Update Server

Patch Management

Patch Management Policy

Workstations and servers owned by the Municipality must have up-to-date (as defined by this policy) operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by the Municipality.

Patches are not flawless and sometimes cause more harm than good. Harmful patches are usually withdrawn or rectified within a week of release. Patches will therefore be downloaded to the WSUS Server daily, but held back for at least a week and then be released to other servers and workstations if it was not withdrawn or if a rectification did not come through during that week.

Workstations

Desktops and laptops must have automatic updates enabled for operating system patches and virus definitions. These updates include Driver updates, Windows updates, OS Security updates, Anti-Virus updates, Back-up Software updates. This is the default configuration for all workstations built by the Municipality. Any exception to the policy must be clearly defined and documented.
The organization will have a centralized WSUS server. This server will download the patches during the night and upload to workstations after approval and release by the ICT Manager.

The organisation will also have a centralised Anti-Virus Package. New virus definitions will be downloaded during the night and uploaded to workstations during the day.
This setup is intended at reducing network bottlenecks.

Servers

Servers must comply with the minimum baseline requirements that have been approved by the Specifications Committee. These minimum baseline requirements define the default operating system level, service pack, hot fix, and patch level required to ensure the security of the asset of the Municipality asset and the data that resides on the system. Any exception to the policy must be clearly defined and documented.

Patch Management

Roles and Responsibilities	The IT Team with support from the External IT Support will manage the patching needs for the Microsoft Windows servers on the network. The External IT Support will manage the patching needs of all workstations on the network. The IT Team will be responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management. The ICT Manager and the Chief Financial Officer (CFO), is responsible for approving any monthly and emergency patch management deployment requests. In the absence of the CFO, the Manager standing in for the CFO will have authority to approve and sign-off these requests. The IT Administrator will keep evidence of patches implemented as well as implemented patches that caused problems and make it available to Management and Internal Audit on request.
Monitoring and Reporting	The IT Administrator is required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Management and Internal Audit upon request.
Enforcement	Implementation and enforcement of this policy is ultimately the responsibility of all employees at the Municipality. Information Security and Internal Audit may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action.
Exceptions	Exceptions to the patch management policy require formal documented approval from the CFO. Any servers or workstations that do not comply with policy must have an approved exception, signed by the CFO.
Disciplinary Actions	Violation of this policy may result in disciplinary action.

Privacy

Introduction

Privacy Policies are mechanisms used to establish the limits and expectations for the users of the Municipality's Information Resources. Internal users should have no expectation of privacy with respect to Information Resources. External users should have the expectation of complete privacy, except in the case of suspected wrongdoing, with respect to Information Resources.

Purpose

The purpose of the Municipality Information Services Privacy Policy is to clearly communicate the Municipality's Information Services Privacy expectations to Information Resources users.

Audience

The Municipality Information Services Privacy Policy applies equally to all individuals who use any of the Municipality's Information Resources.

Ownership

Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of the Municipality are the property of the Municipality.

Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Services (IS): The name of the department responsible for computers, networking and data management.

Web server: A computer that delivers (*serves up*) web pages.

Web page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (Hyper Text Markup Language), which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape Navigator, and Microsoft Internet Explorer.

Website: A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.

IS Privacy Policy

- Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of the Municipality are not private and may be accessed by the Municipality IS employees at any time without knowledge of the IR user or owner.
- To manage systems and enforce security, the Municipality may log, review, and otherwise utilize any information stored on or passing through its IR.
- A variety of third parties have entrusted their information to the Municipality for business purposes, and all workers at the Municipality must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.
- Users must report any weaknesses in the Municipality computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on the Municipality systems for which they do not have authorisation or explicit consent.

Disciplinary Actions

Violation of this policy may result in disciplinary action.

Public Access Privacy Policy	The Municipality web sites available to the general public must contain a Privacy Statement. An example of a good public Privacy Statement follows:

1.2 Web site Privacy Statement on the Use of Information Gathered from the General Public

The following statement applies only to members of the general public and is intended to address concerns about the types of information gathered from the public, if any, and how that information is used.

I. Cookies

A "cookie" is a small file containing information that is placed on a user's computer by a web server. Typically, these files are used to enhance the user's experience of the site, to help users move between pages in a database, or to customize information for a user.

Any information that the Municipality web servers may store in cookies is used for internal purposes only. Cookie data is not used in any way that would disclose personally identifiable information to outside parties unless the Municipality is legally required to do so in connection with law enforcement investigations or other legal proceedings.

II. Logs and Network Monitoring

The Municipality maintains log files of all access to its site and also monitors network traffic for the purposes of site management. This information is used to help diagnose problems with the server and to carry out other administrative tasks. Log analysis tools are also used to create summary statistics to determine which information is of most interest to users, to identify system problem areas, or to help determine technical requirements.

Information such as the following is collected in these files:

Hostname: the hostname and/or IP address of the computer requesting access to the site;

User-Agent: the type of browser, its version, and the operating system of the computer requesting access (e.g., Netscape 4 for Windows, IE 4 for Macintosh, etc.);

Referrer: the web page the user came from;

System date: the date and time on the server at the time of access;

Full request: the exact request the user made;

Status: the status code the server returned, e.g. fulfilled request, file not found;

Content length: the size, in bytes, of the file sent to the user;

Method: the request method used by the browser (e.g., post, get);

Universal Resource Identifier (URI): the location of the particular resource requested. (More commonly known as a URL.);

Query string of the URI: anything after a question mark in a URI. For example, if a keyword search has been requested, the search word will appear in the query string; and

Protocol: the technical protocol and version used, i.e., http 1.0, ftp, etc.

The above information is not used in any way that would reveal personally identifying information to outside parties unless the Municipality is legally required to do so in connection with law enforcement investigations or other legal proceedings.

III. Email and Form Information

If a member of the general public sends the Municipality an e-mail message or fills out a web-based form with a question or comment that contains personally identifying information, that information will only be used to respond to the request and analyse trends. The message may be redirected to another organisation or person who is better able to answer your question. Such information is not used in any way that would reveal personally identifying information to outside parties unless System Administration is legally required to do so in connection with law enforcement investigations or other legal proceedings.

IV. Links

This site may contain links to other sites. The Municipality is not responsible for the privacy practices or the content of such websites.

V. Security

This site has security measures in place to protect from loss, misuse and alteration of the information.

1.3 Contacting the Municipality

If there are any questions about this privacy statement, the practices of this site, or dealings with this website, contact the person in charge of Information Technology.

Supporting Information Reference #	1.3.1.1 This Security Policy is supported by the following Security Policy Standards.
	1.3.2 Policy Standard detail
2	Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
16	Custodian department(s) must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorised and controlled.

Network access

Introduction

The Municipality network infrastructure is provided as a central utility for all users of the Municipality's Information Resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet the Municipality demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the Municipality's Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of the Municipality information.

Audience

The Municipality's Network Access Policy applies equally to all individuals with access to any of the Municipal Information Resources.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the Municipality for management of the Municipality's information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Municipality's information activities, and ensure greater visibility of such activities within the Municipality. The IRM has been given the authority and the accountability by the Municipal Council to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the Municipality. If the Municipality does not designate an IRM, the title defaults to the Municipality's Municipal Manager, and the Municipal Manager is responsible for adhering to the duties and requirements of an IRM.

Network access

Definitions, continued

Information Security Officer (ISO): Responsible to executive management for administering the information security functions within the Municipality. The ISO is the Municipality's internal and external point of contact for all information security matters. This role is currently performed by the Information Technology Administrator.

Information Services (IS): The name of the Municipality department responsible for computers, networking and data management.

Network Access Policy

- Users are permitted to use only those network addresses issued to them by the Municipality IS.
- All remote access (dial in services) to the Municipality will be either through an approved modem pool or via an Internet Service Provider (ISP) using Virtual Private Networking (VPN).
- Remote users may connect to the Municipality Information Resources only through an ISP and using protocols approved by the Municipality.
- Users inside the Municipality firewall may not be connected to the Municipality network at the same time a modem is being used to connect to an external network.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Municipality network without Municipal IS approval.
- Users must not install network hardware or software that provides network services without IS approval.
- Non-Municipal computer systems that require network connectivity must conform to the Municipality's IS Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, The Municipal users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the Municipal network infrastructure.
- Users are not permitted to alter network hardware in any way.

Disciplinary Actions

Violation of this policy may result in disciplinary action.

Network access

Supporting Information	1.3.2.1 This Security Policy is supported by the following Security Policy Standards
Reference #	**Policy Standard detail**
1	IR Security controls must not be bypassed or disabled.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
5	Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.
6	The use of IR must be for officially authorised business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper Authorisation of IR utilization, the establishment of effective use, and reporting of performance to management.
20	External access to and from IR must meet appropriate published Municipality security guidelines.

Server Hardening

Introduction

Servers are depended upon to deliver data in a secure and reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorised access, unauthorised use, and disruptions in service.

Purpose

The purpose of the Municipality's Server Hardening Policy document is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software.

Audience

The Municipality Server Hardening Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security.

Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the Municipality for management of the Municipality's information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Municipality's information activities, and ensure greater visibility of such activities within the Municipality. The IRM has been given the authority and the accountability by the Municipal Council to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the Municipality. If the Council does not designate an IRM, the title defaults to the Municipal Manager and the Municipal Manager is responsible for adhering to the duties and requirements of an IRM.

Vendor: someone who exchanges goods or services for money.

Server Hardening

Definitions, continued

Information Services (IS): The name of the Municipal department responsible for computers, networking and data management.

Server: A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server though it may also be running other client (and server) programs.

Information Security Officer (ISO): Responsible to the executive management for administering the information security functions within the Municipality. The ISO is the Municipality's internal and external point of contact for all information security matters. This role is currently being performed by the II Administrator

Server Hardening Policy

- A server must not be connected to the Municipality network until it is in a IS accredited secure state and the network connection is approved by the Municipality IS.
- The Server Hardening Procedure provides the detailed information required to harden a server and must be implemented for the Municipality IS accreditation. Some of the general steps included in the Server Hardening Procedure include:
  - Installing the operating system from an IS approved source.
  - Applying vendor supplied patches.
  - Removing unnecessary software, system services, and drivers.
  - Setting security parameters, file protections and enabling audit logging.
  - Disabling or changing the password of default accounts.
- The Municipality IS will monitor security issues, both internal to the Municipality and externally, and will manage the release of security patches on behalf of the Municipality.
- The Municipality IS will test security patches against IS core resources before release where practical.
- The Municipality IS may make hardware resources available for testing security patches in the case of special applications.
- Security patches must be implemented within the specified timeframe of notification from the Municipality IS.

Disciplinary Actions

Violation of this policy may result in disciplinary action.

Server Hardening

Supporting Information	**This Security Policy is supported by the following Security Policy Standards.**
Reference #	**Policy Standard detail**
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected.
11	The department which requests and authorises a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian.
12	The IR network is owned and controlled by IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorised and controlled.
17	All departments must carefully assess the risk of unauthorised alteration, unauthorised disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the Municipality is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

Account Management

Introduction

Computer accounts are the means used to grant access to the Municipality Information Resources. These accounts provide a means of providing accountability, a key to any computer security program, for Information Resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of the Municipality's Account Management Security Policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

Audience

The Municipality Account Management Security Policy applies equally to all individuals with authorised access to any of the Municipality Information Resources.

Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Definitions, continued

Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the Municipality. The ISO is the Municipality's internal and external point of contact for all information security matters.

Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system

System Administrator: Person responsible for the effective operation and maintenance of Information Resources, including implementation of standard procedures and controls to enforce an organisation's security policy.

Currently the Information Security Officer, Security Administrator and System Administrator roles are performed by the Information Technology Administrator (ITA).

Account Management

Account Management Policy	• Access to systems will only be granted where there is a clearly established business need, which is consistent with the roles and responsibilities of those granted access. • All accounts created must have an associated request and approval that is appropriate for the Municipality system or service. • All users must sign the Municipality Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an account. • All accounts must be uniquely identifiable using the assigned user name. • All default passwords for accounts must be constructed in accordance with the Municipality Password Policy. • All accounts must have a password expiration that complies with the Municipality Password Policy. • Accounts of individuals on extended leave (more than 30 days) will be disabled. • All new user accounts that have not been accessed within 30 days of creation will be disabled. • Accounts that have not been active for 30 days or more will be disabled. • System Administrators or other designated staff: ❖ are responsible for removing disabling the accounts of individuals that change roles within the Municipality or are separated from their relationship with the Municipality. ❖ must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes. ❖ must have a documented process for periodically reviewing existing accounts for validity. ❖ are subject to independent audit review. ❖ must provide a list of accounts for the systems they administer when requested by authorised Municipality management. ❖ must cooperate with authorized Municipality management investigating security incidents.
Disciplinary Actions	Violation of this policy may result in disciplinary action.

Account Management

Supporting Information Reference #	1.3.2.2 This Security Policy is supported by the following Security Policy Standards. **Policy Standard detail**
1	IR Security controls must not be bypassed or disabled.
2	Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
4	Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organisation. All security violations shall be reported to the custodian or owner department management.
5	Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.
6	The use of IR must be for officially authorised business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper Authorisation of IR utilization, the establishment of effective use, and reporting of performance to management.
7	Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

Supporting Information, continued

1.3.2.3 This Security Policy is supported by the following Security Policy Standards.

Reference #	Policy Standard detail
9	On termination of the relationship with the Municipality users must surrender all property and IR managed by the Municipality. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorised and controlled.
17	All departments must carefully assess the risk of unauthorised alteration, unauthorised disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the Municipality is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

Administrative and Special Access

Introduction	Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.
Purpose	The purpose of the Municipality Administrative/Special Access Practice Standard is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege.
Audience	The Municipality Administrative/Special Access Practice Standard applies equally to all individuals that have, or may require, special access privilege to any the Municipality Information Resources.

Administrative and Special Access

Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the Municipality for management of the Municipality's information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Municipality's information activities, and ensure greater visibility of such activities within the Municipality. The IRM has been given the authority and the accountability by the Municipality Board of Directors to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the Municipality. If the Council does not designate an IRM, the title defaults to The Municipal Manage (MM) and the MM is responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the Municipality. The ISO is the Municipality’s internal and external point of contact for all information security matters.

Information Services (IS): The name of the Municipality department responsible for computers, networking and data management.

Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system.

System Administrator: Person responsible for the effective operation and maintenance of IR, including implementation of standard procedures and controls, to enforce an organisation’s security policy.

Abuse of Privilege: When a user willfully performs an action prohibited by organisational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

Vendor: someone who exchanges goods or services for money.

Administrative and Special Access

Administrative/ Special Access Policy	• The Municipality departments must submit to IS a list of administrative contacts for their systems that are connected to The Municipal network. • All users must sign the Municipality Information Security Employee Declaration before access is given to an account. • All users of Administrative/Special access accounts must have account management instructions, documentation, training, and Authorisation. • Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the Council or designate. • Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account). • Each account used for administrative/special access must meet the Municipality Password Policy. • The password for a shared administrator/special access account must change when an individual with the password leaves the department or the Municipality, or upon a change in the vendor personnel assigned to a Municipality contract. • In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation. (i.e. The password should be stored in a sealed envelope within a safe or at the bank) • When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they: ❖ must be authorised ❖ must be created with a specific expiration date ❖ must be removed when work is complete
Disciplinary Actions	Violation of this policy may result in disciplinary action.

Supporting Information Reference #	1.3.2.4 This Security Policy is supported by the following Security Policy Standards. **Policy Standard detail**
1	IR Security controls must not be bypassed or disabled.
2	Security awareness of personnel must be continually emphasised, reinforced, updated and validated.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
4	Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organisation. All security violations shall be reported to the custodian or owner department management.
5	Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.
6	The use of IR must be for officially authorised business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorisation of IR utilisation, the establishment of effective use, and reporting of performance to management.
7	Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

Supporting Information, continued

1.3.2.5 This Security Policy is supported by the following Security Policy Standards.

Reference #	Policy Standard detail
9	On termination of the relationship with the Municipality users must surrender all property and IR managed by the Municipality. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorised and controlled.
17	All departments must carefully assess the risk of unauthorised alteration, unauthorised disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the Municipality is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

Physical Access

Introduction	Technical support staff, security administrators, system administrators, and others may have Information Resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Resources facilities is extremely important to an overall security program.
Purpose	The purpose of the Municipality Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.
Audience	The Municipality Physical Access Policy applies to all individuals within the Municipality enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Resources Security and data owners.
Definitions	**Information Resources (IR):** any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information. **Information Services (IS):** The name of the Municipality department responsible for computers, networking and data management.
Physical Access Policy	• All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes. • Physical access to all Information Resources restricted facilities must be documented and managed. • All IR facilities must be physically protected in proportion to the criticality or importance of their function at the Municipality. • Access to Information Resources facilities must be granted only to the Municipality support personnel, and contractors, whose job responsibilities require access to that facility. • The process for granting card and/or key access to Information Resources facilities must include the approval of the person responsible for the facility. • Each individual that is granted access rights to an Information Resources facility must complete the appropriate access and non-disclosure agreements.

Physical Access Policy, continued

- Requests for access must come from the applicable Municipality data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility.
- Cards and/or keys must not have identifying information other than a return mail address.
- All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals that change roles within the Municipality or are separated from their relationship with the Municipality
- Visitors must be escorted in access controlled areas of Information Resources facilities.
- The person responsible for the Information Resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the Information Resources facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Disciplinary Actions

Violation of this policy may result in disciplinary action.

Supporting Information Reference #	1.3.2.6 This Security Policy is supported by the following Security Policy Standards Policy Standard detail
1	IR Security controls must not be bypassed or disabled.
2	Security awareness of personnel must be continually emphasised, reinforced, updated and validated.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
4	Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organisation. All security violations shall be reported to the custodian or owner department management.
5	Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected in accordance with their classification.
9	On termination of the relationship with the Municipality users must surrender all property and IR managed by the Municipality. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorised and controlled.
19	IR computer systems and/or associated equipment used for Municipality business that is conducted and managed outside of Municipality control must meet contractual requirements and be subject to monitoring.

Security Training

Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving Municipal security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

Purpose

The purpose of the Security Training Policy is to describe the requirements for ensure each user of the Municipality Information Resources is receives adequate training on computer security issues.

Audience

The Municipality Security Training Policy applies equally to all individuals that use any Municipal Information Resources.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Services (IS): The name of the Municipal department responsible for computers, networking and data management.

Security Training Policy	• All new users must attend an approved Security Awareness training class prior to, or at least within 30 days of, being granted access to any the Municipal information resources. • All users must sign an acknowledgement stating they have read and understand the Municipality requirements as outlined in the computer security policies and procedures. No access will be given to Municipal systems until such acknowledgement is received. The user acknowledgement form should be signed off by each employee at least once a year. • All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect the Municipal information resources. • IS must prepare, maintain, and distribute one or more information security manuals that concisely describe the Municipality information security policies and procedures. • All users must attend an annual computer security compliance in-house training and pass the associated examination. • IS must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.
Disciplinary Actions	Violation of this policy may result in disciplinary action.

Security Training

Supporting Information	**This Security Policy is supported by the following Security Policy Standards**
Reference #	**Policy Standard detail**
2	Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

Portable Computing

Introduction

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

Purpose

The purpose of the Municipality Portable Computing Security Policy is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of the Municipality information.

Audience

The Municipality Portable Computing Security Policy applies equally to all individuals that utilize Portable Computing devices and access the Municipality Information Resources.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the Municipality for management of the Municipality's information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Municipality's information activities, and ensure greater visibility of such activities within the Municipality. The IRM has been given the authority and the accountability by the Municipality Council to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the Municipality. If the Council does not designate an IRM, the title defaults to the Municipality’s Municipal Manager, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

Definitions, continued

Information Security Officer (ISO): Responsible to executive management for administering the information security functions within the Municipality. The ISO is the Municipality's internal and external point of contact for all information security matters.

Information Services (IS): The name of the Municipality department responsible for computers, networking and data management.

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from IR. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and cell phones.

Portable Computing

Portable Computing Policy	• Only the Municipality approved portable computing devices may be used to access the Municipality Information Resources. • Portable computing devices must be password protected. • All remote access (dial in services) to the Municipality must be either through an approved modem pool or via an Internet Service Provider (ISP) using VPN. • A central register must be maintained by the IT function or department responsible for IT of all users with dial-in / remote accesses, also indicating the access authorities to facilitate auditable processes. • To minimise the risk of compromising security, all users of the remote access services must receive training before access is allowed. The training should include what is allowed and what is not allowed during sessions. • In order to ensure compliance in terms of software, hardware and security requirements, the computer used for the remote access should be provided by the municipality. The use of private (home) computers may only be allowed if based on a valid business need and must be processed as a deviation from this policy. The manager/department responsible for IT security shall maintain a central register of all the deviations. • Non-Municipality computer systems that require network connectivity must conform to the Municipality IS Standards and must be approved in writing by the Municipal ISO. • The remote client (computer used to access the municipality's network) must have anti-virus software and the correct level of security patches as prescribed by the IT function from time to time. A process must be formulated by the IT function to ensure the regular update of the software/patches. • The user who has signed for the receipt of any portable computing device remains fully responsible for the device until it has been returned and signed off by the ISO. • Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.
Disciplinary Actions	Violation of this policy may result in disciplinary action.

Supporting Information	1.3.2.7 This Security Policy is supported by the following Security Policy Standards
Reference #	**Policy Standard detail**
1	IR Security controls must not be bypassed or disabled.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
5	Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.
7	Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
12	The IR network is owned and controlled by IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
20	External access to and from IR must meet appropriate published Municipality security guidelines.

Password

Introduction

User authentication is a means to control who has access to an Information Resource system. Controlling the access is necessary for any Information Resource which needs to be protected in terms of the **Protection of Personal Information** Act 4 of 2013 (POPI) Act. Access gained by a non-authorised entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to the Municipality.

Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- Something you know – password, Personal Identification Number (PIN).
- Something you have – Smartcard.
- Something you are – fingerprint, iris scan, voice.
- A combination of factors – Smartcard and a PIN.

Purpose

The purpose of the Municipality Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the Municipality user authentication mechanisms.

Audience

The Municipality Password Policy applies equally to all individuals who use any Municipality information resource.

1.3.3 Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the Municipality for management of the Municipality's information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Municipality's information activities, and ensure greater visibility of such activities within the Municipality. The IRM has been given the authority and the accountability by the Municipal Council to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the Municipality. If the Council does not designate an IRM, the title defaults to the Municipal Manager and the Municipal Manager is responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO): Responsible to the executive management for administering the information security functions within the Municipality. The ISO is the Municipality’s internal and external point of contact for all information security matters.

Information Services (IS): The name of the Municipality department responsible for computers, networking and data management.

Password: A string of characters which serves as authentication of a person’s identity, which may be used to grant, or deny, access to private or shared data.

Strong Passwords: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, identity number, and so on.

Password

Password Policy

The following account policy settings must be implemented on all Windows servers.

Restriction	Setting
Maximum password age	Expires in 30 Days
Minimum password age	1 day
Minimum password length	At Least 8 Characters
Password history length	Remember 24 Passwords
Account Lockout	Enabled
Lockout accounts after	3 bad attempts
Counter resets after	1440 Minutes
Lockout duration	0 Minutes (Forever)
Password Complexity	Enabled
Password Reverse Encryption	Disabled
Default passwords shipped with operating systems/program products for use during system and product installation/setup	Change as soon as possible
Password Never Expires	May not be enabled for any user ID's
Password Never Expires Exception	Admin Password for all services (AV, Management, Backup etc.)

- All passwords, including initial passwords, must be constructed and implemented according to the following Municipality IR rules:
  - Complexity requirements: A password must be a combination of alpha (alphabetical letters), numeric characters (whole numbers) and special symbols (!@#$) of which there must be at least one capital letter, one lower case letter, one numeric characters and one special symbol.
  - it must not be anything that can easily tied back to the account owner such as: user name, id number, nickname, relative's names, birth date, etc.
  - it must not be dictionary words or acronyms.
  - Passwords should not be written down unless protected in some or other form (e.g. by using a sort of encryption and locking it away).
  - The authentication server/system will maintain a list of up to 24 previous passwords used per user and each new password should contain at least 3 changes. The objective of this rule is to prevent users re-using the same password over and over.
  - Accounts must be locked out after 3 incorrect attempts.
- Stored passwords must be encrypted.
- User account passwords must not be divulged to anyone. The Municipality IS, and IS contractors will not ask for user account passwords.

- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with the Municipality (Currently, this paragraph does not apply as tokens are not used however it has been retained in the policy should the use of tokens be implemented in the future).
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Policy for the sake of ease of use.
- Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Municipality ISO. In order for an exception to be approved there must be a procedure to change the passwords.
- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device. Whenever the user leaves their desk and the PC is switched on, it is essential that the user ALWAYS 'lock' their screen by pressing 'Ctrl Alt Delete' (for NT/2000/XP operating systems) and then enter to confirm that they wish to 'lock' their workstation. Remember that the user will need their password to sign on. Users of Windows 95 and 98 desktops should use the screensaver password function to activate after 5 minutes of inactivity.
- Locking the screen not only prevents someone else from using the PC, which is logged on in the user's name, but it also prevents someone from reading sensitive information on the screen.
- Password change procedures must include the following:
  - Authenticate the user before changing password (i.e. users should personally request changes);
  - Change to a strong password; and
  - The user must change password at first login.
- In the event passwords are found or discovered, the following steps must be taken:
  - Take control of the passwords and protect them
  - Report the discovery to the Municipality IT Administrator
  - Transfer the passwords to an authorised person as directed by the Municipality ISO.

Password Guidelines

System Value/Parameter	Setting
Required action for: • Creating new user ID's • Password resets	Set an initial password and force the user to change it. The check box 'User must change password at next login' must be selected.
Guest account which allows system login without entry of a specific password	Disable
Administrator account	Rename to a more secure name or have a long complex password with a minimum of 15 characters.

- Passwords must contain a mix of upper and lower case characters and have at least 2 numeric characters. The numeric characters must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (!@#$%^&*_+=?/~`;:,<>|\).
- Passwords must not be easy to guess and they:
  - must not be your Username;
  - must not be your employee number;
  - must not be your name;
  - must not be family member names;
  - must not be your nickname;
  - must not be your identity number;
  - must not be your birthday;
  - must not be your license plate number;
  - must not be your pet's name;
  - must not be your address;
  - must not be your phone number;
  - must not be the name of your town or city;
  - must not be the name of your department;
  - must not be street names;
  - must not be makes or models of vehicles;
  - must not be slang words;
  - must not be obscenities;
  - must not be technical terms;
  - must not be school names, school mascot, or school slogans;
  - must not be any information about you that is known or is easy to learn (favorite - food, color, sport, etc.);
  - must not be any popular acronyms;
  - must not be words that appear in a dictionary; and
  - must not be the reverse of any of the above.
- Passwords must not be shared with anyone.
- Passwords must be treated as confidential information.

Creating a strong password	• Combine short, unrelated words with numbers or special characters. For example: eAt42peN
	• Make the password difficult to guess but easy to remember.
	• Substitute numbers or special characters for letters. (But do not just substitute) For example:
	  • Livefish - is a bad password.
	  • L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed.
	  • l!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable.

Disciplinary Actions	Violation of this policy may result in disciplinary action.

Supporting Information Reference #	1.3.3.1 This Security Policy is supported by the following Security Policy Standards **Policy Standard detail**
1	IR Security controls must not be bypassed or disabled.
2	Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
4	Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organisation. All security violations shall be reported to the custodian or owner department management.
5	Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.
9	On termination of the relationship with the Municipality, users must surrender all property and IR managed by the Municipality. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorised and controlled.

Acceptable Use

Introduction

Information Resources are strategic assets of the Municipality that must be managed as valuable corporate resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Audience

The Municipality Acceptable Use policy applies equally to all individuals granted access privileges to any Municipality Information Resources.

Ownership of Electronic Files

Electronic files created, sent, received, or stored on Information Resources owned, leased administered, or otherwise under the custody and control of the Municipality are the property of the Municipality .

Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of the Municipality are not for private use and may be accessed by the Municipality IS employees at any time without knowledge of the Information Resources user or owner (This is subject to approval from appropriate management only). Electronic file content may be accessed by appropriate personnel who have been granted the necessary authority by the information owner.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the Municipality for management of the Municipality's information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Municipality's information activities, and ensure greater visibility of such activities within the Municipality. The IRM has been given the authority and the accountability by the Municipal Council to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the Municipality. If the Council does not designate an IRM, the title defaults to the Municipal Manager, and the Municipal Manager is responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the Municipality. The ISO is the Municipality’s internal and external point of contact for all information security matters.

User: An individual or automated application or process that is authorised access to the resource by the owner, in accordance with the owner’s procedures and rules.

Information Resources Acceptable Use Policy

- Users must report any weaknesses in the Municipality computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on the Municipality systems for which they do not have Authorisation or explicit consent.
- Users must not divulge Dialup or Dial back modem phone numbers to anyone.
- Users must not share their Municipality User account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and Authorisation purposes.
- Users must not make unauthorised copies of copyrighted software. This includes Movies or Videos that are not work related.
- Users must not use non-standard shareware or freeware software without the Municipality Information Resources management approval unless it is on the Municipality standard software list.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorised Municipality user access to a Municipal resource; obtain extra resources beyond those allocated; circumvent the Municipality computer security measures.
- The access provided by the municipality is not to be used to access any material of a sexual, violent, destructive or potentially harmful nature. The system must be used in a moral and ethical manner. Access to and storage of pornographic material is strictly forbidden.
- The account may not be used to conduct any illegal activities. It is the responsibility of management to ensure that the security policies are effectively communicated to users in order to establish accountability.
- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, the Municipality users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on the Municipality Information Resources.
- The computer must be kept updated with the latest municipal accepted anti-virus agent. The municipality employees can obtain a copy from the IT department/function.
- The Municipality Information Resources must not be used for personal benefit.

Acceptable Use

- Users must not intentionally access, create, store or transmit material which the Municipality may deem to be offensive, indecent or obscene.
- Access to the Internet from a Municipality owned, home based, computer must adhere to all the same policies that apply to use from within the Municipality facilities. Employees must not allow family members or other non-employees to access the Municipality computer systems.
- Unless specifically specified, the municipality does not offer technical support for personal (home) computers.
- Users must not otherwise engage in acts against the aims and purposes of the Municipality as specified in its governing documents or in rules, regulations and procedures adopted from time to time.
- Users will be held accountable for actions committed under the specific user profile.

Incidental Use

As a convenience to the Municipality user community, incidental use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to the Municipality approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to the Municipality.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, the Municipality.
- Storage of personal email messages, voice messages, files and documents within the Municipality's Information Resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on the Municipality Information Resources are owned by the Municipality, may be subject to open records requests, and may be accessed in accordance with this policy without the consent of the user.

Disciplinary Actions

Violation of this policy may result in disciplinary action.

Supporting Information	This Security Policy is supported by the following Security Policy Standards.
Reference #	**Policy Standard detail**
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
6	The use of IR must be for officially authorised business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorisation of IR utilization, the establishment of effective use, and reporting of performance to management.
7	Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected in accordance with their classification.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorised and controlled.
21	All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. IS reserves the right to remove any unlicensed software from any computer system.

Supporting Information, continued	This Security Policy is supported by the following Security Policy Standards.
Reference #	**Policy Standard detail**
22	The Municipality through IS reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, movies, video's, instant messengers, pop email, music files, image files, freeware, and shareware.

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

The purpose of the Computer Virus Detection Policy is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup.

Audience

The Municipality Computer Virus Detection Policy applies equally to all individuals that use any the Municipality Information Resources.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the Municipality for management of the Municipality's information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Municipality's information activities, and ensure greater visibility of such activities within the Municipality. The IRM has been given the authority and the accountability by the Council of the Municipality to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the Municipality. If the Council does not designate an IRM, the title defaults to the Municipal Manager, and the Municipal Manager is responsible for adhering to the duties and requirements of an IRM.

1.3.4 Definitions, continued

Information Security Officer (ISO): Responsible to executive management for administering the information security functions within the Municipality. The ISO is the Municipality's internal and external point of contact for all information security matters.

Information Services (IS): The name of the Municipality department responsible for computers, networking and data management.

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

Trojan Horse: Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network, using otherwise-unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Server: A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Security Incident: In information operations, an assessed event of attempted entry, unauthorised entry, or an information attack on an automated information system. It includes unauthorised probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

E-mail: Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.

Virus Detection Policy	• All workstations whether connected to the Municipality network, or standalone, must use the Municipality IS approved virus protection software and configuration. • The virus protection software must not be disabled or bypassed. • The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software. • The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates. • Each file share server attached to the Municipality network must utilise the Municipality IS approved virus protection software and setup to detect and clean viruses that may infect file shares. • Each E-mail gateway must utilize the Municipality IS approved e-mail virus protection software and must adhere to the IS rules for the setup and use of this software. • Every virus that is not automatically cleaned by the virus protection software is put into quarantine and automatically uploaded to the Antivirus Lab for deconstruction and patch release.
Disciplinary Actions	Violation of this policy may result in disciplinary action.

Supporting Information	**This Security Policy is supported by the following Security Policy Standards**
Reference #	**Policy Standard detail**
1	IR Security controls must not be bypassed or disabled.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
6	The use of IR must be for officially authorised business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorisation of IR utilisation, the establishment of effective use, and reporting of performance to management.
7	Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorised and controlled.

Supporting Information, continued	**This Security Policy is supported by the following Security Policy Standards**
1.3.4.1.1 Reference #	**1.3.4.1.1.1 Policy Standard detail, continued**
21	All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The IRM through IS reserves the right to remove any unlicensed software from any computer system.
22	The Municipality through IS reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

Vendor Access

Introduction

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can in certain instances remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors, they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to the Municipality.

Purpose

The purpose of the Municipality Vendor Access Policy is to establish the rules for vendor access to the Municipality Information Resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of the Municipality information.

Audience

The Municipality Vendor Access Policy applies to all individuals that are responsible for the installation of new Information Resources assets, and the operations and maintenance of existing Information Resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Vendor: someone who exchanges goods or services for money.

Vendor Access

Vendor Access Policy

- Vendors must comply with all applicable Municipality policies, practice standards and agreements, including, but not limited to:
  - Safety Policies
  - Privacy Policies
  - Security Policies
  - Auditing Policies
  - Software Licensing Policies
  - Acceptable Use Policies
- Vendor agreements and contracts must specify:
  - The Municipality information the vendor should have access to.
  - How the Municipality information is to be protected by the vendor in line with the **Protection of Personal Information Act 4 of 2013 (POPI ACT).**
  - Acceptable methods for the return, destruction or disposal of the Municipality information in the vendor's possession at the end of the contract.
  - The Vendor must only use the Municipality information and Information Resources for the purpose of the business agreement
  - Any other Municipality information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- The Municipality will provide an IS point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
- Each vendor must provide the Municipality with a list of all employees working on the contract. The list must be updated and provided to the Municipality within 24 hours of staff changes.
- Each on-site vendor employee must acquire a Municipality identification badge that will be displayed at all times while on the Municipality premises. The badge must be returned to the Municipality when the employee leaves the contract or at the end of the contract.
- Each vendor employee with access to the Municipality sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate Municipality personnel.
- If vendor management is involved in the Municipality security incident management the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable Municipality change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate Municipality management.

Vendor Access

Vendor Access Policy, continued

- All vendor maintenance equipment on the Municipality network that connects to the outside world via the network, telephone line, or leased line, and all the Municipality IR vendor accounts will remain disabled except when in use for authorised maintenance.
- Vendor access must be uniquely identifiable and password management must comply with the Municipality Password Practice Standard and Admin/Special Access Practice Standard. Vendor's major work activities must be entered into a log and available to the Municipality management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to the Municipality or destroyed within 24 hours.
- Upon termination of contract or at the request of the Municipality, the vendor will return or destroy all the Municipality information and provide written certification of that return or destruction within 24 hours.
- Upon termination of contract or at the request of the Municipality, the vendor must surrender all the Municipality Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented and authorised by Municipality management.
- Vendors are required to comply with all the Municipality auditing requirements, including the auditing of the vendor's work.
- All software used by the vendor in providing service to the Municipality must be properly inventoried and licensed.

Disciplinary Actions

Violation of this policy may result in disciplinary action.

Supporting Information Reference #	1.3.4.2 This Security Policy is supported by the following Security Policy Standards **1.3.5 Policy Standard detail**
1	IR Security controls must not be bypassed or disabled.
2	Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
4	Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organisation. All security violations shall be reported to the custodian or owner department management.
5	Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.
6	The use of IR must be for officially authorised business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorisation of IR utilization, the establishment of effective use, and reporting of performance to management.
7	Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

1.3.5.1.1 Supporting Information, continued	**This Security Policy is supported by the following Security Policy Standards**
Reference #	**1.3.6 Policy Standard detail**
9	On termination of the relationship with the Municipality users must surrender all property and IR managed by the Municipality. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorised and controlled.
17	All departments must carefully assess the risk of unauthorised alteration, unauthorised disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the Municipality is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

Network Configuration

Introduction

The Municipality network infrastructure is provided as a central utility for all users of the Municipality Information Resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the Municipality Network Configuration Security Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of the Municipality information.

Audience

The Municipality Network Configuration Policy applies equally to all individuals with access to any the Municipality Information Resource.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the Municipality for management of the Municipality's information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Municipality's information activities, and ensure greater visibility of such activities within the Municipality. The IRM has been given the authority and the accountability by the Council to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the Municipality. If the Council does not designate an IRM, the title defaults to the Municipal Manager, and the Municipal Manager is responsible for adhering to the duties and requirements of an IRM.

Network Configuration

Definitions, continued

Information Security Officer (ISO): Responsible to executive management for administering the information security functions within the Municipality. The ISO is the Municipality's internal and external point of contact for all information security matters.

Information Services (IS): The name of the Municipality department responsible for computers, networking and data management.

Network Configuration Security Practice Standards

- The Municipality Information Services owns and is responsible for the Municipality network infrastructure and will continue to manage further developments and enhancements to this infrastructure
- To provide a consistent network infrastructure capable of exploiting new networking developments, all cabling must be installed by the Municipality IS or an approved contractor.
- All network connected equipment must be configured to a specification approved by the Municipality IS.
- All hardware connected to the Municipality network is subject to the Municipality IS management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of the Municipality IS.
- The Municipality network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by the Municipality IS.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by the Municipality IS.
- All connections of the network infrastructure to external third party networks are the responsibility of the Municipality IS. This includes connections to external telephone networks.
- **Firewall** – A firewall will be installed to protect the municipalities internal networks and systems from external attacks and penetration attempts. The creation of a demilitarised zone is preferred, but not mandated. This policy may be revised should the municipality experience a high incidence of penetration attempts. The firewall should be configured to provide at least the following:
  - ❖ Network Address Translation (NAT).
  - ❖ Proxy services.
  - ❖ Port blocking and control.
  - ❖ Virus attack protection.
  - ❖ WWW management features.
  - ❖ Logging of audit information.
  - ❖ Custom rule formulation and configurations.
- The use of departmental firewalls is not permitted without the written authorisation from the Municipality IS.

- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Municipality network without IS approval.
- Users must not install network hardware or software that provides network services without the Municipality IS approval.
- Users are not permitted to alter network hardware in any way.

Disciplinary Actions

Violation of this policy may result in disciplinary action.

Supporting Information

1.3.6.1 This Security Policy is supported by the following Security Policy Standards.

Reference #	Policy Standard detail
12	The IR network is owned and controlled by IS. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. IS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
15	All changes or modifications to IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.
19	IR computer systems and/or associated equipment used for the Municipality business that is conducted and managed outside of the Municipality control must meet contractual requirements and be subject to monitoring.
20	External access to and from IR must meet appropriate published the Municipality security guidelines.

Electronic Mail Policy

Introduction

This Policy clarifies the position of the Municipality with regard to electronic mail. It also defines new policy and procedures where existing policies do not specifically address issues particular to the use of electronic mail.

The Municipality recognizes that principles of freedom of speech and privacy of information hold important implications for electronic mail and electronic mail services. The Municipality affords electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications. This Policy reflects these firmly-held principles within the context of the Municipality's legal and other obligations.

The Municipality encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail without the holder's (as defined in ECT Act, 25 of 2002 Act, 25 of 2002) consent. It also abides by the Protection of Personal Information Act 4 of 2013 (POPI Act). Nonetheless, subject to the requirements for Authorisation, notification, and other conditions specified in this Policy, the Municipality may deny access to its electronic mail services and may inspect, monitor, or disclose electronic mail (i) when required by and consistent with law; (ii) when there is substantiated reason (as defined in ECT Act, 25 of 2002 Act, 25 of 2002) to believe that violations of law or of the Municipality policies listed in Appendix A have taken place;.

Cautions:

Users should be aware of the following:

- Both the nature of electronic mail and the public character of the Municipality's business (see Caution 2 below) make electronic mail less private than users may anticipate. For example, electronic mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. The Municipality cannot routinely protect users against such eventualities.
- Electronic mail, whether or not created or stored on the Municipality equipment, may constitute a the Municipality record subject to disclosure under the ECT Act, 25 of 2002 Act, 25 of 2002 or other laws, or as a result of litigation. However, the Municipality does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Act, other laws concerning disclosure and privacy, or other applicable law.
- Users of the Municipality electronic mail services also should be aware that the ECT Act, 25 of 2002 Act, 25 of 2002 and other similar laws jeopardize the ability of the Municipality to guarantee complete protection of *personal* electronic mail resident on the Municipality facilities**.**
- The Municipality, in general, cannot and does not wish to be the arbiter of the contents of electronic mail. Neither can the Municipality, in general, protect users from receiving electronic mail they may find offensive. Members of the Municipality staff,

Electronic Mail Policy

however, are strongly encouraged to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.

- There is no guarantee, unless "authenticated" mail systems are in use, that electronic mail received was in fact sent by the purported sender, since it is relatively straightforward, although a violation of this Policy, for senders to disguise their identity.
- The Municipality prohibits any use of encryption unless prior Authorisation from the Chief Executive Officer is obtained

Purpose

The purpose of the Municipality Email Policy is to establish the rules for the use of the Municipality email for the sending, receiving, or storing of electronic mail. And to ensure that:

- electronic mail services are used in compliance with those rules;
- Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail;
- and Disruptions to the Municipality electronic mail and other services and activities are minimized.

Audience

The Municipality Email Policy applies equally to all individuals granted access privileges to any the Municipality information resource with the capacity to send, receive, or store electronic mail.

This Policy applies both to electronic mail in its electronic form and printed copies of email. Electronic mail messages, therefore, in either their electronic or printed forms, are subject to those other policies, including provisions of those policies regarding retention and disclosure.

This Policy applies equally to transactional information (such as email headers, summaries, addresses, and addressees) associated with email records as it does to the contents of those records.

Electronic Mail Policy

Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Electronic Mail Policy

Email Policy

A. Allowable Use

In general, use of the Municipality electronic mail services is governed by policies that apply to the use of all the Municipality facilities. In particular, use of the Municipality electronic mail services is encouraged and is allowable subject to the following conditions:

- **Purpose**. Electronic mail services are to be provided by the Municipality in support of the public service mission of the Municipality, and the administrative functions that support this mission.

- **Users**. Users of the Municipality electronic mail services are to be limited primarily to the Municipality staff.

- **Restrictions**. The Municipality electronic mail services may not be used for:
  - Sending email that is intimidating or harassing.
  - Using email for conducting personal business.
  - Using email for purposes of political lobbying or campaigning.
  - Violating copyright laws by inappropriately distributing protected works.
  - Posing as anyone other than oneself when sending email, except when authorised to send messages for another when serving in an administrative support role.
  - The use of unauthorised e-mail software.
  - Unlawful activities.
  - Commercial purposes not under the auspices of the Municipality.
  - Personal financial gain.
  - Or uses that violate other the Municipality policies or guidelines.

- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
  - Sending or forwarding chain letters.
  - Sending unsolicited messages to large groups except as required to conduct Municipality business.
  - Sending excessively large messages
  - Sending or forwarding email that is likely to contain computer viruses.
  - Sending "letter-bomb," that is, to resend the same email repeatedly to one or more recipients to interfere with the recipient's use of email.

- **Representation**. Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Municipality or any division of the Municipality unless appropriately authorised

(explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the Municipality. An appropriate disclaimer is: "These statements are my own, and not those of the Municipality."

- **False Identity**. Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Municipality or any unit of the Municipality unless appropriately authorised (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the Municipality.
- The Municipal disclaimer should be as: **"**The views expressed in this email are, unless otherwise stated, those of the author and not those of SENQU Municipality or its management. The information in this e-mail is confidential and is intended solely for the addressee recipient(s) only. Access to this e-mail by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted in reliance on this, is prohibited and may be unlawful. Whilst all reasonable steps are taken to ensure the accuracy and integrity of information and data transmitted electronically and to preserve the confidentiality thereof, no liability or responsibility whatsoever is accepted if information or data is, for whatever reason, corrupted or does not reach its intended destination**"**

- **Personal Use**. The Municipality electronic mail services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not: (i) directly or indirectly interfere with the operation of computing facilities or electronic mail services within the Municipality; (ii) burden the Municipality with noticeable incremental cost; or (iii) interfere with the email user's employment or other obligations to the Municipality.

B. Security and Confidentiality

- All user activity on the Municipality Information Resources assets may be subject to logging and review.
- Individuals must not send, forward or receive confidential or sensitive Municipality information through non-municipal email accounts. Examples of non-municipal email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).
- Individuals must not send, forward, receive or store confidential or sensitive Municipality information utilising non-municipal accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers and cellular telephones.
- The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or

policy, including this Policy, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorised access. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters.

- The Municipality prohibits employees and others from "seeking out, using, or disclosing" without Authorisation "personal or confidential" information, and requires employees to take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties or otherwise.
- Notwithstanding the previous paragraph, users should be aware that, during the performance of their duties, network and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of the Municipality email services, and on these and other occasions may inadvertently see the contents of email messages. Except as provided elsewhere in this Policy, they are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. One exception, however, is that of systems personnel (such as "internet service providers") who may need to inspect email when re-routing or disposing of otherwise undeliverable email. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt internet service providers from the prohibition against disclosure of personal and confidential information of the previous paragraph, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable email to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the email has been inspected for such purposes.
- The Municipality attempts to provide secure and reliable email services. Operators of the Municipality electronic mail services are expected to follow sound professional practices in providing for the security of electronic mail records, data, application programs, and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, however, the security and confidentiality of electronic mail cannot be guaranteed. Furthermore, operators of email services have no control over the security of email that has been downloaded to a user’s computer. As a deterrent to potential intruders and to misuse of email, email users should employ whatever protections (such as passwords) are available to them.
- Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies that can be retrieved. Systems may be "backed-up" on a routine or occasional basis to protect system reliability and integrity, and to

prevent potential loss of data. The back-up process results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail.

C. Archiving and Retention

The Municipality may maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up automatically on every user's workstation.

Disciplinary Actions

Violation of this policy may result in disciplinary action.

Supporting Information

1.3.6.2 This Security Policy is supported by the following Security Policy Standards.

Reference #	Policy Standard detail
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
6	The use of IR must be for officially authorised business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance to management.
7	Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected in accordance with their classification.

Software Licensing Policy

Introduction

End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

Purpose

The purpose of the Software Licensing Policy is to establish the rules for licensed software use on the Municipality Information Resources.

Audience

The Municipality Software Licensing Policy applies equally to all individuals that use any the Municipality Information Resources.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the Municipality for management of the Municipality's information resources. The designation of an information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Municipality's information activities, and ensure greater visibility of such activities within the Municipality. The IRM has been given the authority and the accountability by the Council to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the Municipality. If the Council does not designate an IRM, the title defaults to the Municipal Mayor, and the Municipal is responsible for adhering to the duties and requirements of an IRM.

Information Services (IS): The name of the Municipal department responsible for computers, networking and data management.

Vendor: someone who exchanges goods or services for money.

Software Licensing Policy

Software Licensing Policy	• The Municipality provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities. • Third party copyrighted information or software, that the Municipality does not have specific approval to store and/or use, must not be stored on the Municipality systems or networks. Systems administrators will remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s). • Third party software in the possession of the Municipality must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.
Disciplinary Actions	Violation of this policy may result in disciplinary action.

Software Licensing Policy

Supporting Information	This Security Policy is supported by the following Security Policy Standards
Reference #	**Policy Standard detail**
1	IR Security controls must not be bypassed or disabled.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected.
9	On termination of the relationship with the Municipality users must surrender all property and IR managed by the Municipality. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
21	All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The IRM through IS reserves the right to remove any unlicensed software from any computer system.

Version Control Document

Policy	Version	Revised Date	Effective Date
Senqu IS Security Policy	V2_12_02_2009	22/02/2010	01/03/2012
Senqu IS Security Policy	V3_08_04_2015	08/04/2015	01/07/2015
Senqu IS Security Policy	V4_05_05_2016	20/05/2016	01/07/2016
Senqu IS Security Policy	V5_07_05_2017	07/05/2017	01/07/2017

Senqu Municipality Approval and Sign-Off

Date of Approval by Council: 28 July 2017
Resolution Number: 020/OCM/17

_____ _____

MM YAWA **DATE**
MUNICIPAL MANAGER

Recommendation:
That the report be noted,
That the ICT Security Policies be approved by Council.