The purpose of this policy is to outline the direction, scope and approach to secure management of Information Assets and Information Systems within the Municipality. Its intention is to protect the information assets, and any ICT assets which create, process, store, view or transmit information against unauthorised use or accidental modification, loss or release.

ICT SECURITY POLICY

Setsoto Local Municipality

APPROVAL

DOCUMENT:	**INFORMATION COMMUNICATION TECHNOLOGY SECURITY POLICY**		
Copy Number:	**MASTER COPY**		
Compiled by:	Rakesh Bugwandeen	**Reviewed by:**	Rakesh Bugwandeen
Compilation Date:	31.07.2011	**Review Date:**	21 January 2020
Version:	V.03	**Version:**	V. 06
Distribution:	All	**Classification:**	Confidential
Document Release Approval		**Document Acceptance**	
Releasing Authority: Office of the Municipal Manager	ICT, Communication & CRM	**Acceptance Authority:**	Council
Date Released:		**Date Accepted:**	
	Signature:		**Signature:**

DOCUMENT REVISION HISTORY

VERSION	DATE	NAME	DESCRIPTION
V. 01	31 July 2007	Rakesh Bugwandeen	Draft
V. 01	30 September 2007	Rakesh Bugwandeen	Finalised
V. 02	31 March 2010	Rakesh Bugwandeen	Reviewed (No Changes)
V. 03	31 March 2011	Rakesh Bugwandeen	Reviewed (No Changes)
V. 04	31 March 2017	Tshepiso Motsima	Reviewed (Changes Occurred)
V. 05	09 October 2019	Rakesh Bugwandeen	Reviewed (No Changes)
V.06	21 January 2020	Rakesh Bugwandeen	Reviewed (No Changes)

DOCUMENT REVIEW CONTROL

This Municipality's Information and Communications Technology policy shall be subjected to the review process after 1 year of its operation. It shall remain in operation during the review process. Changes to it while it is still in operation shall be made after consultation with the Municipal Manager as the Accounting Officer and be approved by the Council. Such changes shall ensure that the organisation's aims and objectives will be adhered to, and no function shall be disabled and /or ignored, and any initiative to commit in altercating or changing the document shall be authorised by the Municipal Manager or his / her delegated nominee. This policy may also be reviewed at the instance of material changes necessitated by legislative development, governing frameworks and applicable regulations.

Contents

1. INTRODUCTION.

Setsoto Local Municipality (SLM) is situated in the eastern part of the Free State Province within the regional boundaries of the Thabo Mofutsanyana District Municipality. It was established in terms of Section 14 of the Local Government: Municipal Structures Act 117 of 1998 and was published in Provincial Gazette No. 184 dated 28 September 2000. The Municipality is a category B Municipality. It covers the towns of Clocolan, Marquard, Senekal and Ficksburg which also serves as the administrative capital of the Municipality. According to Census 2011 Municipal Fact Sheet, published by Statistics South Africa (Report No. 03-01-58), the Municipality is home to more than 112 000 people.

The Municipality firstly acknowledges that it has an obligation to serve the needs of the communities within its jurisdiction, and as such an effective and efficient Information and Communications Technology (ITC) policy will enable it to meet its objectives as outlined in its strategic plan. Secondly, it has an obligation to ensure that information security for all Information Technology data, equipment and processes in its domain of ownership and control, and whatsoever outsourced beneficially to the Municipality's exposure and use is well managed and maintained. It is however, recognised that various departments and divisions within the Municipality provide services that relate to information security, both directly and indirectly. It is therefore expected that there will be collaboration between these divisions and the ICT Manager regarding the generation of standards and the implementation of the policy.

In light of the Control Objectives for Information and Related Technology (COBIT 5), Information Technology Infrastructure Library (ITIL), International Standards Organisation (ISO) 27001 and ICT Governance on King III Report frameworks the Municipality is mindful of the fact that ICT policies are not just an ICT-only activity, but expands to incorporate ICT principles inclusive of the end to end business processes that ensures a better coverage and cooperation across the institution, by which responsibilities and authorities have been clearly defined and correctly articulated.

The ICT is an important tool in ensuring that the employees of the Municipality are able to execute their duties effectively, efficiently and diligently. However, like any other tool, it is imperative that it is managed and maintained effectively so that the Municipality can be able to derive maximum value from the utilisation of its ICT assets. The Municipality has a responsibility to ensure that its ICT assets are well maintained and managed while they meet needs of the users for them to be effective. This implies that as the Municipality is committed to continuously improve the capacity of its personnel by providing all the qualifying staff members with the necessary ICT equipment and resources for them to be able to perform their duties to the best of their abilities for the benefit of the people of Setsoto in general.

This policy defines the processes that are going to be used to ensure effective usage and management of the ICT resources. It is the Municipality's intention to provide vibrant and well-articulated ICT services to equip individuals in their respective designations within the institution to be able to execute their various duties effectively, directly and indirectly. Among other milestones, these processes will be undertaken to reduce duplication of controls across different Departments of

the institution, and also to provide consistent approach to address business and operational requirements responding to individual attributes, thus taking into cognisance the integrity, ethical values and competence in a manner that warrants a clear communication of the policy which is understood, supported and accepted by everyone within the Municipality.

Therefore, the intensity of this document shall be viewed and accepted in light of the efforts that defines the implementation of a comprehensive governance and management system of the technological resources in recognition of the organisational structures, culture, ethics and behaviour, services, infrastructure and applications. The ICT policy has been developed to ensure that it is managed in a way that protects the privacy, confidentiality and integrity of the information of the Municipality that is at the disposal of the ICT users, while also properly maintaining the ICT assets of the Municipality.

2. PURPOSE OF THE POLICY.

The purpose of this policy is to outline the direction, scope and approach to secure management of Information Assets and Information Systems within the Municipality. Its intention is to protect the information assets, and any ICT assets which create, process, store, view or transmit information against unauthorised use or accidental modification, loss or release. It will firstly set out the principles and guidelines that will determine the acceptable use of the Municipality ICT assets and resources. Secondly, it will ensure adequate protection and preservation of all information in either print or electronic form which is owned, generated or is in the possession of the Municipality. It also seeks to provide the institution with an information and communication system security policy encompassing appropriate levels of security through standards and guidelines, which will be characterised by;

- **Confidentiality** – ensuring the accessibility of information to employees authorised to have access.
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods.
- **Availability** – ensuring that only authorised users have access to information and associated assets when required.
- **Compliant use** – ensuring that the municipality meets all its legal and contractual obligations.
- **Responsible use** – ensuring that appropriate controls are put in place so that the user have access to accurate, relevant and timely information that they are able to utilise responsibly.

The provisions of the policy will in parallel with all the regulations be binding on the employees and staff of the Municipality, whether contracted, employed (permanent or temporary), and no one shall be exempted from the rules and regulations in as much as its purpose is to maintain staff accountability for the protection of information resources.

3. OBJECTIVES OF THE POLICY.

The adoption and the subsequent implementation of this policy by the Municipality will seeks to ensure a stable, safe and secure a networking environment that will directly and indirectly serve the broader community of the Setsoto, stakeholders, contractors as well as its very own staff in the employ. As a result, the Municipality seeks to:

- Achieve strategic goals and realise business benefits through effective usage of its ICT resources.
- Achieve operational excellence through reliable and efficient application of technology.
- Protect the investment in the ICT infrastructure**.**
- Maintain ICT-related risks within acceptable levels.
- Manage and organise information more easily**.**
- Optimise the costs of ICT services and technology bound by the governing frameworks and regulations.

- Comply with ever-increasing relevant legislation, regulations, contractual agreements and policies.
- Ensure responsibility and accountability by the users of the Municipality's assets and resources.

4. DEFINITION OF ICT SECURITY POLICIES.

ICT Security Policies are referred to as mandatory management instructions indicating a predetermined course of action or a way of handling a problem or situation. They are part of the Municipality's regulations and special approval is required and it has to be under very exceptional circumstances when an employee wishes to take a course of action that is likely to transgress or is non-compliant with policy as approved by the Municipality. Policies are distinct from procedures and standards. They address the general means of addressing a specific problem. Standards cover details such as implementation steps, system design concepts, software interface specifications and software algorithms. On the other hand procedures are specific operational steps or manual methods that employees must utilise to achieve a certain goals.

5. DEFINITION OF MANAGEMENT AND ORGANISATIONAL RESPONSIBILITIES.

The Municipality ICT Sub-Committee together with the designated personnel are bound to report to the ICT Steering Committee. The subcommittee's main functions is to review the status of Municipality's physical, computer and network security, review and monitor work which is related to computer and network security incidents, establish, maintain, implement, administer and interpret organization-wide ICT security policies, guidelines, and procedures. The Steering committee will be responsible for authorisation followed by the judgment of the results pertaining to major projects dealing with computer and network security, approve new and/or modified policies, guidelines and procedures.

The Municipality's ICT unit will perform ICT risk assessment, prepare ICT security action plans, evaluate information security products and perform any other activities necessary to assure a secure ICT environment. There is a need to conduct investigations into any alleged computer or network security compromises, incidents or problems, and these must be immediately reported to the relevant ICT Unit. The ICT Manager together with the ICT officers are responsible for acting as local information systems security coordinators. These individuals are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer. They also are responsible for reporting all suspicious computer and network-security-related activities to the IT Unit System administrators and also implement the requirements of this and other information systems security policies, guidelines, and procedures.

6. INFORMATION CLASSIFICATION.

Sensitive Information on the Municipality systems will be classified and allocated in the following manner:

Process Outline	Highly Restricted	Confidential	Internal Use Only	Public
Classified Information	Operating Systems Software. Database Management System	Customer information. Customer accounts. Application Software.	Intranet. E-mail. Information Security procedure manuals, strategy, job description and terms of service.	Website information Tender Documents.
Information Owners	Corporate Services ICT Manager	Operations. Financial Management.	ICT Manager	Head of Departments.

7. ROLES AND RESPONSIBILITIES.

The Municipality's personnel that will be responsible for all ICT and related assets will have the following responsibilities:

Manager: ICT	Accountable for the usage of ICT resources.
ICT Personnel	Responsible for the integrity and security of data on the server and shared drive, as well as the backing up of data.
Users	Responsible for the integrity, security and the backing up of municipal data held on their individual workstations.
Service Providers	Manages the application systems that store municipal data, and also ensure its integrity and perform backups of all data belonging to the municipality.

System Administrators	Responsible for establishing, communicating and enforcing procedures that promote information security.

8. SCOPE OF APPLICATION OF THE POLICY.

This policy shall be applicable to any person, recognised and authorised to be the user of resources and information assets within the Municipality, utilising ICT resources and facilities in pursuing the Municipality's goals and strategic objectives. Therefore, it shall govern the conditions of acceptable use of ICT resources installed and configured for use. It provides standards for users in the management and use of ICT resources, as well as to ensure that the users are accountable for protecting Municipality's information assets by properly classifying assets in terms of their confidentiality, integrity, availability and non-repudiation.

9. LEGISLATIVE FRAMEWORK.

The guiding principles used in developing this draft policy document which will be referred to as the Setsoto Local Municipality Information and Communications Technology (ICT) Policy upon approval by the Municipality, were sourced from the following documents, legislation, frameworks, standards and best practices.

- The Constitution of the Republic of South Africa, Act 108 of 1996
- Electronic and Communications Act 36 of 2005
- Preferential Procurement Policy Framework Act 5 of 2000
- Municipal Structures Act 117 of 1998
- Municipal Systems Act 32 of 2000
- Computer Misuse Act of 1990
- Local Government: Municipal Performance Regulations, 2006
- Municipal Finance Management Act, 2003 (Act No. 56 of 2003) : Sec 62 (2)(C)(i)
- State Information Technology Agency (SITA) Act 1998 as amended 2002
- Minimum Information Security Standards, NIA, 2003
- Control Objectives for Information and Related Technology (COBIT) 5, ISACA, 2012
- Information Technology Infrastructure Library (ITIL)
- ISO 27001
- KING III Report, 2009
- SALGA: Municipal ICT Governance Guidelines, 2012

10. ICT RISK MANAGEMENT POLICY.

Purpose:

The purpose of the ICT Management Policy is:

- To ensure that the staff (frequent users of resources in place) is aware of the appropriate risk management procedures that are mandatory for all the components of the ICT information system lifecycle within the municipality. Giving due cognisance to the critical role of the ICT across operational areas of the institution, this places a great onus on the ICT in particular and the municipality in general to identify risks, manage risks and develop continuity plans.
- To affirm the Municipality's commitment to appropriate risk management policy that will mitigate against any possible risks.
- To help integrate risks management practices across the Municipality.
- To help foster an environment where staff and all other users of the municipality's ICT services assume responsibility for managing risks.

Scope of Application:

This policy will be applied in conjunction with the ruling frameworks and governance methodologies to help ensure that a consistent approach to risks identified across the municipality's ICT system and operations will be dealt with by communicating, mitigating and escalating major risks issues, as well as incorporating risk management principles and objectives into strategic, operational and resource planning.

10.1. ICT Risk Management Policy Objectives

The objectives of the ICT Risk Management Policy are to ensure that:

- Appropriate risk management processes are adopted for all phases of the information system lifecycle.
- The Municipality's ICT office adopts risk management in the approval, review and control of all ICT projects.
- Risk management processes are put in place are transparent and includes appropriate and timely involvement of stakeholders and decision makers.
- Risk management is used proactively to identify and classify the risks in pursuing ICT strategic and operational objectives.
- Risk management policies and procedures cover specialised areas such as the commercial business activities and also take into account the human and cultural factors.

10.2. Types of Risks:

The types of risks the Risk Management Policy seeks to address are the following:

Hardware	• Invalidation of hardware due to technical changes obsolete). • Loss of System availability (lacks of preventative maintenance) • Unlimited physical access into computer room.
Operating Systems	• Invalidation of the Operations system due to technical change or poor supplier support. • Loss of system availability (no up to date backups). • Poor system performance (no regular checking of log files and system error message files). • Loss of system systems integrity (unlimited access to the root prompt).
Database Management Systems	• Loss of business data confidentiality (limited access control). • Loss of system availability (regular backups must include DBMS). • Loss of data (no backups). • Lack of business data integrity (allow access to DBMS). • Poor systems performance (no checking of database bottlenecks). • Excessive use of storage (compromising storage). • Loss of availability to interrogate data (compromising access to databank). • Limited or no regular system audits.
Change Management Systems	• Unpredictable results due to change (upgrades). • Unable to revert back to initial status due to change (no backups of system before change implemented). • Service availability can be reduced by change. • Security and integrity of data can be compromised by change.

	• Business continuity plans may be invalidated by change. • Change can be costly.
Problem Management	• Failure to treat the problems. • Problems not prioritized. • No reporting of problems. • System and data security compromised by consultant access to original level. • Resolution of problems costly or slow.
Asset Management	• The quantity, type and location of computer assets is unknown. • Inaccurate assets register. • Asset management responsibility unclear. • Acquisition of assets costly. • No benefits on disposal of assets when they are obsolete.
Capacity Management	• Insufficient disk space. • Costly excess disk storage. • Inaccurate storage calculations. • Unexpected business trends impacting on available disk space. • Additional storage not made available when needed (file system configuration nor well planned).
Access Control	• Invalidation of system software (lack of supplier support). • Loss of system availability (uncontrolled physical access). • Poor system performance (service level agreements with users). • Loss of system software integrity (compromise of confidentiality).
Networks	• Change/corruption of data during transmission. • Confidential information read during transmission. • Network performance does meet user requirements. • Network services not available when required (line down). • Unavailable network management software.
Desktops/Notebooks or Laptops	• Integrity of business data is lost or its confidentiality violated due to viruses. • Integrity of application systems program code is lost due to unauthorized access. • Illegal copies of software are in use.

	• Theft of desktop/mobile computing systems. • Insufficient desktop/mobile computing facilities available in the event of a business interruption. • Management and maintenance of desktop too costly.
Computer Operations and environment	• Batch processing not completed. • Operator work too many hours and are unfit. • Few operators engaged on shifts. • Interruption to operations due to power cuts, fire etc.

10.3. Risk Management Process (RMP).

The RMP is the process that will be followed in identifying the risks so that they could be mitigated.

10.3.1. Risk Identification:

This is the most important process because any unidentified risks cannot be mitigated. In this instance the primary focus should be on real threats and less on theoretical ones.

10.3.2. Risk Analysis:

This is done so as to develop an understanding on the type of risk the institution is facing. The process examines any given situation, checking for obvious deficits according to professional experience or even common sense.

10.3.3. Risk Evaluation:

This process entails some form of evaluation by quantifying the results and comparing them with acceptable risk criteria. This is in preparation for dealing with the risk.

10.3.4. Risk Management:

It is at this stage where a number of options are being considered to be able to deal with the identified risk appropriately. This is where the risk mitigation strategy is being put in place.

11. ACCESS CONTROL POLICY.

Purpose:

The purpose of the Access Control Policy is:

- To communicate the need for access control.
- To define the correct use and management access controls within the Municipality.
- To ensure the security and confidentiality of the information it processes on behalf of its clients, stakeholders and employees.
- To establish specific requirements for protection against unauthorised access.
- To create an ICT infrastructure that will foster data sharing without compromising ICT infrastructure resources.

Scope of Application:

This policy shall apply to all ICT resources owned and leased by the municipality, information system and network domains, users (staff, contractors, interns and authorised third party commercial service providers), Local and remote connections to the network domain (LAN/WAN and Wi-Fi).

11.1. Access Control Requirements

The development of access control policy by the Municipality is aimed at protecting information and its ICT resources from loss or unauthorised access. It will certainly incorporate balancing the need to impose restrictions to prevent access against the need to provide access to meet the Municipality's business needs. The Municipality's ICT division should ensure that all users are uniquely identifiable on key ICT systems, and authentication mechanisms must be used to identify users. Access shall be controlled in such a manner that users will be assigned the least privileges required to execute their daily job functions, or whenever they are required to have such access granted to them.

11.2. User Access Management

To contingently manage user privileges of the Municipality's resources, the IT office shall put in place procedures for creating, modifying and suspending user accounts and/or privileges. In this regard, administrators and privileged users shall follow the same user account management procedures, and regular management reviews of all accounts and related privileges that would be performed by the relevant departmental managers.

11.2.1. User Account Creation and Termination:

User accounts created through the Active Directory and application systems should be created through the completion of forms (to be approved by the relevant line Manager) for new users. Access to the systems must be authorised by the owner of the system and such access, inclusive of the appropriate access rights must be recorded in an *Access Control List* and the forms that are be

filled in for the user access forms. Such documentation shall at all costs be regarded as highly confidential. The user accounts will be disabled or deactivated at the specified time period to block the misuse of the account, or in such a case where there is a suspected multiple incorrect log-in onto the system.

In the event that administration of the system is performed by a third party, consultant or a business division outside of the Municipality's ICT unit, the Chief Financial Officer (CFO), ICT Manager and/or Municipal Manager shall ensure that the policies and procedures are implemented. In the event that an employee is leaving and/or released from duties by the Municipality, the HR Department shall file a written notice with the ICT department via proper channels (e-mail), thereupon which the *Network User Termination Form* will be completed and signed by the user.

11.2.2. Logical Access and Access Rights Review:

Access to the computer network and systems shall only be granted in accordance with the employee's job requirements, and the user access rights will also be approved by the staff member who shall so be authorised such as data owners. ICT personnel shall from time to time (on an annual basis) make user access rights reports to account for the review and signoff of the access as confirmation that access is still aligned to the user job functions. ICT Unit shall confirm necessary amendments, in the event that access right have been changed and/or there have been a suspicion that a violation of user privileges or access rights may have taken place.

11.3. Network Access Controls

The Municipality will put in place a network that is adequately designed and configured to deliver high performance and reliability to address the needs of the institution, and also provides a high degree of access control and a range of privilege restrictions. This will enable the Municipality to ensure that the network is strictly controlled to prevent unauthorised access. In the midst of implementing the control processes, the Municipality's systems shall be operated and administered using documented procedures in a manner which is both efficient, but also effective in enforcing and protecting against misuse of privileges granted to users and their access rights.

11.3.1. Access Management:

New users will be registered on the system by submitting a written application with a list of services, programmes and/or data to which access may be required, fully signed and authorised by the respective line manager of the department to which the user will report to. No simultaneous access or multiple logging-in by the same user in different stations is allowed, except in cases where prior authorisation is sought, and a valid reason if given by the line manager of the respective department. File and directory permissions must be granted to specific users or groups only. This will allow the user to use a file or directory in a particular way.

11.3.2. Positioning of Peripherals and Devices

Network points must, as far as possible be segregated from one another, be in a in a knowledge centre, lab or training room. Internet traffic should be logged to identify the computer and/or user. Users may not leave workstations unattended while still logged onto the system. In the event where this arises, the activity within the station will be automatically monitored and traced, upon which such connection will be terminated within a period of 10 minutes.

11.3.3. Remote Access and Third-Party Access

Users seeking remote access must be restricted to the minimum services and functions necessary for the business purpose. Remote access shall be authenticated using strong authentication methods which will require the user to log on the system with their current assigned credentials i.e. normal used ID and password. Third-party access shall adhere to remote access policies and procedures where applicable. Third-party access to the Municipality's information and data processing facilities must be controlled, documented and approved. All third-party account must be revoked once the employee's contract is terminated or have resigned from the municipality. The Municipality may, without prior notice, immediately terminate any network connection with third party systems not meeting requirements.

11.4. Applications and Operating Systems

This policy defines roles and responsibilities pertaining to software licensing and the use of prescribed operating systems as it is owned by the Municipality, and the preservation thereof. Incorrect software licencing and/or use could lead to actions being taken against the Municipality or the individuals in question, All the computers and Notebooks deemed to be at the ownership of the Municipality shall be installed with software licensed for the Municipality's use, and upon case in which the Desktop or Notebook crashes, the correct formatting procedures of operating systems shall be adhered to, to format and reload/install the software again. The Municipality is responsible for managing all the licenses and other software under its control.

11.4.1. Applications Regulatory Framework

The installation and use of any kind of software and/or Operating Systems is not allowed if it violates the license agreement with a specific vendor, and as such, it must be uninstalled from the Municipality's computer environment and systems without delay. All software on the Municipality's computers is protected by copyright laws, thus commercial software purchased by the Municipality is authorised for the Municipality's use only and must be utilised in accordance with the contractual agreements and copyright laws governing the relationship between the Municipality and the vendor.

11.5. Mobile Computing / Wireless

The use of mobile computers (notebooks and Laptops) for business and personal uses shall be guided by the standards and policies. Reasonable care and judgement shall be required, and be in compliance with the Municipality's ICT policies, and as required through the terms and conditions of applicable software license agreements.

The user will accept responsibility and take precautions with the mobile computer and shall adhere to the policy governing the use and the control of such assets. For access purposes, a user seeking to connect to the network wirelessly shall not be exempted from the provisions to have the computer connected through a security approved firewall, and deployed by the relevant ICT office.

11.6. Password Management

A password is a convenient and easy method of authentication for users entering a computer system. The system simply requires the user to present something he / she knows as a proof that he is actually who he claims to be. This is easily implemented, but at the same time the password

approach is subject to a number of security threats. The following are common security risks where a legitimate user may lose his or her password:

I. **Over the shoulder attack:** when a person types in his or her password, someone might be able to observe what is being typed and as a result steal the password by looking over the person's shoulder, or by indirect monitoring using a camera.
II. **Brute-force attack:** because a password has a finite length, usually 8 alphanumeric characters, an attacker can use programs that automatically generate passwords, trying all possible combinations until a valid password is found. With recent advances in computing power, the time needed to execute a successful brute force attack has dropped considerably.
III. **Sniffing attack:** when a password is sent over a network, it could be captured by network sniffing tools if the network channel is not properly encrypted. In addition, certain malicious tools (such as a keylogger) might be able to capture a user's password when the password is typed in during the authentication process.
IV. **Login spoofing attack:** this is where an attacker sets up a fake login screen that is similar in look-and-feel to the real login screen. When a user logins to the fake screen, his password will be recorded or transmitted to the attacker.

All these attacks, if successful, can help unauthorised users harvest the passwords of legitimate users. Systems using passwords as the only authentication method will be unable to differentiate whether the holder of the password is a valid user or not

The Municipality enjoys much discretion in terms of the granting of access as well as the management of passwords to offset the complexity and the hassle of having users misusing their privilege by having their log-in details easily accessed or cracked to access the system. Therefore, the Municipality's employees and users using the institutions ICT resources and facilities are responsible for the integrity and confidentiality of passwords allocated. User details must be created and changed frequently as the policy governs, thus disabled and later deleted when the user in question resigns. The password management process should include:

- Secure delivery of initial and temporary password.
- Immediate forced password change.
- Positive identification procedures in emergency situations.
- Positive acknowledgement of password receipt

11.6.1. Password, user ID and Access Rights Administration

Formal standards for password management, user ID's and user access rights should be in place and implemented. Controls should be in place to provide:

I. Reasonable assurance that the use of system utilities is limited to authorized individuals and monitored.
II. Reasonable assurance that access to program source code is limited to properly authorized individuals.
III. Reasonable assurance that sensitive systems identified are isolated appropriately.
IV. Adequate guidance for end user responsibility for password management should be in place and operating effectively. Passwords should comply with the following

- Passwords should be at least 8 characters long -Password changing should be enforced with a minimum frequency of every 30 days.
- Intruder detection should be enabled to out further login attempts after 3 failed attempts.
- The timeout period before the login counter is reset should be 1 hour, and the account should be locked for at least 2 minutes in the event of 3 failed attempts. -Where possible within the Network Operating System the following should also be required:
- Password re-use should be prevented for an agreed number of changes.
- A mixture of alphanumeric and numeric characters or a complete pass phrase should be required.
- There should be a list of banned 'trivial' passwords, enforced automatically be given to any additional security needs of the organisational network and systems, as the need may arise.
- Passwords should be reset, by completing a password reset form. This form should be signed by the user and approved by the manager/supervisor.

12. INTRUSION, DETECTION AND REPORTING POLICY.

Purpose:

The purpose of this policy is to protect the confidentiality of any data that may be stored on the physical and/or mobile computers, and also to protect the Municipality's network from being infected by any hostile software.

Scope of Application:

This policy covers every host on the Municipality's network and the overall data network including every path that such data may travel, that is not on the internet. The paths covered in this policy also include the Municipality's wireless networks.

12.1. Event Reporting

This is the process in which the events/incidents must be detected, reported and resolved. This stage will depict all the necessary steps which the event/incident will go through within the unit, and the manner in which the calls are logged for resolution. For this purpose, the Municipality has established a helpdesk that will manage ICT related support requirements, including third parties that are given access to its network.

12.2. Personnel Responsible for Managing Events and Issues Reporting Protocol:

Role	Responsibility
ICT Manager	Plan for the resolution of incidents and problems in a timely manner.
ICT Technicians	Ensure that they respond to service requests within the agreed-upon times.
ICT Helpdesk Support	Record and assign all incoming calls to available or appropriate technician.

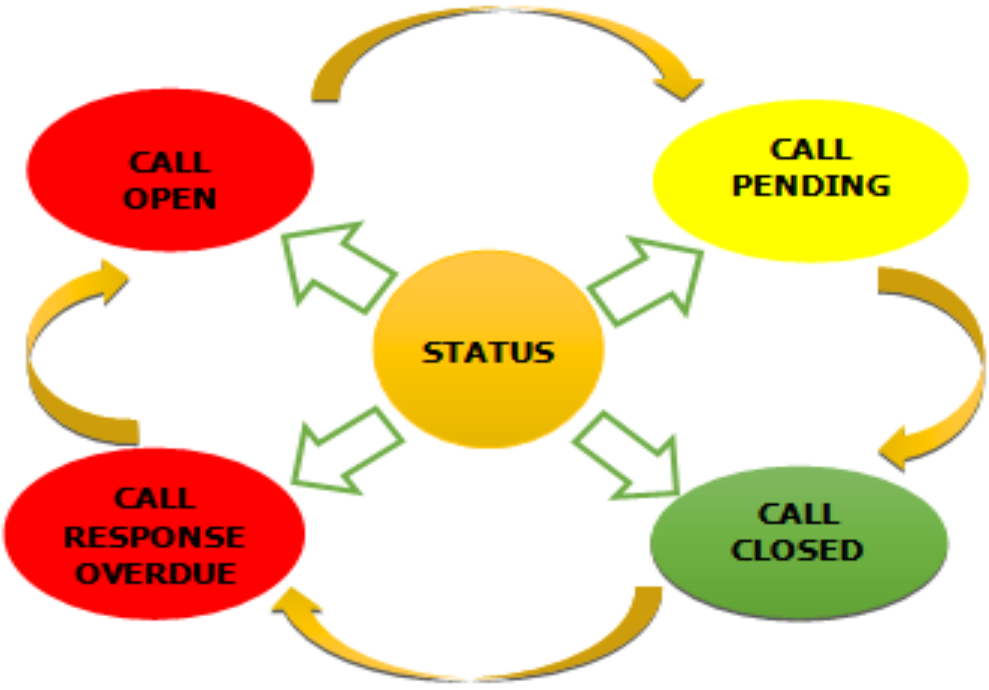
A user calling the ICT Helpdesk must be in front of his/her desktop computer or laptop from which they are logging a call from. This will assist the IT Technician to determine whether to connect to the computer remotely or physical attend to the issue reported. Incidents and job requests are formally managed through a staged process to conclusion, and the objectives of the Incident Management Lifecycle (IML) is to restore the service as promptly as possible to meet Service Level Agreements (SLA). Problem Management deals with resolving the underlying cause of one or more incidents. The focus of problems management is to resolve the root cause of errors and to find permanent solutions. The emphasis is more on the problem resolution rather than the speed of the resolution.

12.3. Incident Detecting and Recording:

The requests for issues with regard to events and detection must be made through telephone, email or walk-in. This is the centralised process by which all the employees are required to be familiar with. The person taking the call must capture relevant details into the Helpdesk call logging spreadsheet or system. These are:

- ✓ Requestor Name:
- ✓ Type of request:
- ✓ Description of the Request:
- ✓ Time of Request:
- ✓ Reference Number of the Request to be assigned:
- ✓ Status of the Call:
- ✓ Call priority Status:

The calls logged must be given a unique number (job request reference number) to allow tracking and follow up. This must be provided to the User, call requestor after the call has been logged. Calls are given statuses as follows;



Call Status	Definition
Open	A call has been logged and a reference number has been issued.
Pending	User is contacted and more information requested.
Resolved	A call has been satisfactorily responded to.
Closed	User is satisfied with the answer/solution to the issue, no more work needs to be done on the job request/ticket.
Response over due	User has logged a call and has not received any answer or notification within 2 working days (> 24 hours since a call was logged).

12.3.1. Out of Compliance and Incidence Response Procedures:

In this instance the procedures that will be followed are the following:

- **Point of Contact:**
  - Service Desk or any other designated official
  - Service providers through the above procedure
  - Imminent notification triggered by monitoring tool(e-mail)
  - System configuration to warn the intruder that they violated your system security for deterrent measures.
  - Always call back the notifier or the person asking about the attack to ensure the call is not a fake or hoax.

- **Immediate Action:**
  - Determine the nature and scope of the violation, the potential damage, how many computers are affected, and if multiple site are involved and sensitive data at risk.

- **Intrusion:**
  - Guarantee the integrity of any mission critical
  - Systems
  - Isolate point of entry in order to stop further attacks
  - Determine where the attack originated
  - Check the operating system audit logs for intrusion details.
  - Restore system to order if possible
  - Involve law enforcement and take legal action, if appropriate
  - Take legal action against the attacker
  - Avoid negative publicity

- **Virus Attack:**
  - Isolate the affected computers
  - Determine how the virus was introduced into the system.

- **Post Incidence Analysis:**

- This process document the event for future reference, where it happened, how it happened, who was contacted, what action was taken to bring the system back to operation.

12.3.2. Vulnerability Identification and Prioritisation

Many devices in an environment provide supporting functions to the Municipality, but have no direct impact to critical information and data. Therefore, this section deals with processes where the Municipality identifies and prioritise exposures and vulnerabilities in order to isolate those that will have the greatest impact, and deploy its limited resources in the most effective manner as possible.

12.3.3. Classification and Prioritisation:

Calls are classified to allow for the appropriate allocation into the different ICT technicians. Call classification is as follows:

I. Passwords
II. Software
III. Hardware
IV. Telephone
V. Printer
VI. Network
VII. Electricity meters
VIII. Application systems

To determine the priority of incidents or requests, consideration is given to the category and the impact which this has to the business. As such the following priorities would be made:

Priority	Criteria	Response Time	Completion
Urgent	>5 users affected, mission critical with less workaround available. e.g: E-mails, Network connectivity, servers and conferencing systems.	Immediate per call	3 hours maximum
High	<5 users affected, and no workaround.	4 hours maximum	1 day (24 hrs.)
Medium	<5 users affected, and workarounds available.	1 working day	3 working days
Low	No effects on productivity or unsupported software. A service not requiring immediate attention. e.g.: monitor showing black and white instead of colour, or CD player has no sound.	3 working days	5 working days

Support is usually categorised into 1st, 2nd and 3rd line support, which means that;

- **1st Line:** support provided by the help of the help desk technician i.e. passwords, printers, telephone connections.
- **2nd Line:** support provided by ICT technician onsite i.e. laptop and desktop, electricity meter systems.
- **3rd Line:** highly technical problems such as network and server problems.

12.3.4. Investigations and Diagnosis:

ICT Manager must ensure that all incidents, service requests and problems are appropriately recorded to allow for investigations of the root cause of recurring problems. Outcomes of such analysis must be recorded into a known error database to enable the quick resolution of incidents and problems in the future. Where significant problems have occurred, investigations made must be recorded and this must also contribute to the overall database. A root cause report detailing all the work done towards making a diagnosis must be compiled and kept on file for future reference.

12.3.5. Reporting:

ICT Office must be able to produce a monthly report on the following to enable trend analysis:

- Recurring problems.
- Number of open problems.
- Number of resolved, but not closed.
- Percentage resolved within the required time.

12.4. Security Event Management

Security devices such as firewalls and intrusion detection systems, most systems on a typical network are capable of generating security events. Examples of security events include authentication events, audit events, intrusion events, and anti-virus events, and these events are usually stored in operating system logs, security logs or database tables. The primary purpose is to safeguard the institution against the risks on security policies and Municipality's business regulations. It is required that security events be monitored and that security logs be reviewed to identify security issues, as this will ensure a consistent collection, transformation, storage, monitoring and analysis of security events. Systems or a device to be monitored falls into one of the following categories:

12.4.1. Security Systems:

This includes systems and devices that perform security function on the network. For example, authentication systems, firewalls, network intrusion detection and prevention systems (IDS/IPS), virtual private network devices (VPNs), host-based intrusion detection systems (HIDS), wireless security devices, and anti-malware systems

12.4.2. Business Critical Systems:

This covers those systems that are important for running the network. For example, mail servers, DNS servers, web servers, authentication servers. When establishing which infrastructure systems are most critical, try to determine what the business impact would be if the system was unavailable. This category of system also includes more traditional network devices such as routers, switches and wireless network devices.

12.4.3. Critical Infrastructure Systems:

This includes those systems that are important for running the network. For example, mail servers, DNS servers, Web servers, authentication servers. When establishing which infrastructure systems are most critical, try to determine what the business impact would be if the system was unavailable. This category of system also includes more traditional network devices such as routers, switches, and wireless network devices.

13. OPERATING SYSTEMS SECURITY CONTROLS

Security facilities at the operating system level should be used to restrict access to computer resources. These facilities should be capable of the following:

(a) identifying and verifying the identity, and if necessary the terminal or location of each authorised user;
(b) recording successful and failed system accesses;
(c) providing appropriate means for authentication and ensuring quality passwords through use of a password management system;
(d) where appropriate, restricting the connection times of users; *and*
(e) Where justified by the business risk, other access controls methods, such as *challenge-response*.

13.1. Automatic terminal identification:

Automatic terminal identification should be considered to authenticate connections to specific locations and to portable equipment. This is a technique that can be used if it is important that the session can only be initiated from a particular location or computer terminal. It may be necessary to apply physical protection to the terminal so that the security of the terminal identifier can be maintained.

13.2. Terminal log-on procedures:

Access to information services should only be attainable via a secure log-on process. The procedure for logging into a computer system must be designed to minimise the opportunity for unauthorised access. The log-on procedure should therefore disclose the minimum information about the system, in order to avoid providing the unauthorised user with unnecessary assistance. A good log-on procedure should:

(a) Not display system or application identifiers until the log-on process has been successfully completed;
(b) Display a general notice that the computer system should only be used by authorized users;
(c) not provide help messages during the log-on procedure that would aid an unauthorized user;
(d) Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;
(e) Limit the number of unsuccessful log-on attempts allowed (three is recommended) and consider:
    I. recording unsuccessful attempts;
    II. forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization; *and*

III. disconnecting data link connections.

(f) Limit the maximum and minimum time allowed for the log-on procedure; if exceeded, the system should terminate the log-on; *and*

(g) display the following information on completion of a successful log-on:

I. date and time of the previous successful log-on; *and*

II. details of any unsuccessful log-on attempts since the last successful log-on.

13.3. User identification and authentication:

All users (including technical support staff, operators, network administrators, systems programmers and data base administrators) must have a unique user identity (*username*) for their personal and sole use so that activities can subsequently be traced to the responsible individual. User identities must give no indication of the user's privilege level. In exceptional circumstances, where there is a clear business or operational justification, the use of a shared user identity for a group of users or a specific job *may* be permitted. Approval by Municipal Manager shall be documented for such cases and one of the users assigned the shared identity shall be nominated to maintain the associated password and be held accountable for the integrity of the user identity and password. A shared identity may only confer READ access privileges.

14. SYSTEMS ACQUISITIONS AND DEVELOPMENT POLICY.

Purpose:

The purpose of the systems and development policy is to communicate formal processes and procedures for procurement that satisfies and meets established business's functional and technical requirement and is in accordance with the Municipality's technology direction.

Scope of Application:

This policy is applicable to provide maximum access to ICT resources and to carefully steward Setsoto Local Municipality's computing support resources, thus giving focus on carefully layered IT goals such as meeting current minimum standards at the workspace of every staff member (computer standards may vary somewhat by user based on discipline, designation and task-specific needs).

The objective of the Municipality is mainly to carry out procurement of ICT products and services in a way that;

- Ensures value for money.
- Maintains the highest standards of integrity.
- Is completely neutral.
- Manages risks.
- Is consistent with government requirements such as Public Finance Management (PFMA) Act etc.

The Municipality acknowledges the need for its procurement practices to encourage greater innovation, reduce costs to business and redress any unfair advantage to particular sections of the market.

14.1. Systems Acquisitions

Acquisition may imply purchasing or rental of equipment. Purchased equipment may have extended warranties that provide for maintenance to be done on site by the companies the equipment was purchased from. Equipment that does not have an extended warranty normally has a year, and possibly, a two year carry-in warranty. In such cases, the Municipality has to take the items to the supplier for repairs or replacement. Hired equipment is normally maintained / repaired by the company supplying the equipment for the duration of the rental contract.

14.1.1. ICT Procurement Framework:

Purchasing of computer hardware and software facilities is mainly done through the normal Municipality's supply chain procedures, and the ICT unit provides the specifications to ensure that the equipment sourced meets the standards and compatible in order to be connect of the

institution's network and supported by the ICT staff. All ICT equipment shall be replaced at the end of their lifecycle (approximately 4 years) or when one or more of the following criteria is met:

I. The item has reached its end-of-life.
II. The item is out of warranty and has become uneconomical to repair.
III. The item is no longer supported by the manufacturer.
IV. The software or application is not compatible with the hardware.

14.1.2. Guidelines for Resource Procurement: Software, Hardware and other Peripherals:

ICT Unit must utilise their capital budget to purchase computers. Therefore, newly acquired units, will then be delivered to the ICT office for configuration for use on the network. Issuing of computers to personnel in the department is based on the work requirements as well as the position of the official in question. Therefore, a request for either a laptop or desktop must first be approved by the Municipal Manager and sufficiently motivated by the Head of Department or Senior Manager of the relevant Unit or Department.

14.2. Systems Development Life Cycle

The life cycle determines the manner in which to ensure when an application is required, redeveloped or upgraded, and whether such a process is economically viable to undertake and that all relevant challenges and needs are taken into account.

14.2.1. Custom Software Application:

When custom application software is considered for the Municipality, care should be taken that it is economically the best option available due to the nature and timeframe of the development of custom applications. It should also be considered that the nature of such expenditure is not always viable for such a small environment but would be best suited for larger environments and organisations with larger operations. The IT Manager should investigate other alternatives in such a case and see where off-the-shelf software cannot be adapted or configured by using macros to perform the same task(s) as are needed from the custom application. If such an application does exist it would be better to reconfigure or use macros than to redevelop such an application.

The Municipal Manager should also ensure that the development of an application includes the application itself and not just a user fee or license to use the program for a period of time. This is common practice with outsourced system development companies (consultant and vendors) that withdraw in the end leaving the institution without an application and a bigger problem than before. The software that is chosen should adhere to all the security and safety precautions implemented on the network to safeguard against disaster or data corruption. If it cannot, the system should be changed or relevant security procedures should be put in place. Should this be done at too high a cost, then the system may not be worth having, especially if it nullifies all security on the network.

15. OPERATIONS PROCEDURES.

Purpose:

The purpose of the operating procedures is to:

- Standardise the methodology in which the facilities will be operated in response to the regulations in place.
- Provide guidance for computer support and operations to promote the continued use and correct operation of a computer system with an emphasis to harness the availability, confidentiality and the integrity of the systems.

Scope of Application:

This operating procedures applies to the Users (staff whether permanent, contractual, temporary or interns) using either personal or institutionally provided equipment connected locally or remotely to the network of the Municipality.

15.1. Programme Change Management Procedures

All changes to the hardware, operating systems and/or application software shall be requested in writing by the user of the system and approved in writing by the:

- ICT official that shall be authorised from the division where the change is to be made
- ICT Manager / official within the ICT unit.
- Specific Manager of the ICT component (Software Developer, Testing Engineer or Network engineer).
- ICT Steering Committee.

Such changes shall only be effected in line with the national and provincial standards, or the ruling guideline by the governing framework or practise, where such arrangement exists, and the change shall be tested prior implementation.

In cases where significant changes are made to any system that, if not executed successfully, may render the system to fail or be redundant, the system shall be backed up prior to such change being made. When the change agent in question restores the action of change from the backup, he/she shall test the reliability of restoring prior to implementation of the change.

15.2. Email and Messaging Procedures

Users are urged to be careful when opening e-mails and email attachments from senders that are not known or emails that were not expected. Should there be any suspicions of this arising, and the user is not sure what to do, IT office must be consulted as soon as possible or ask IT Helpdesk for support or delete the message. Municipality's email systems in general provide limited message

security, therefore, users should show good judgement concerning the transmission of sensitive messages. Email messages routed over public networks, such as the internet, should contain public information only. Misrepresenting, obscuring, spoofing, supressing or modifying a user's identity or any electronic communication system is forbidden. Users are also responsible for regularly reviewing proxy access to their mailbox and calendars.

15.3. Third Party Management Procedures

As part of the Municipality's function in terms of the service roll-out, third parties (vendors, agents or consultants) are often contracted to provide services to the institution. Therefore, agreement with a third party for the use of their services / products must not interfere with existing agreements but rather enhance the prevailing agreements and their related services. Agreements must be established for the exchange of information, and software, between the Municipality and any third party.

Proposed agreements with third parties must be drawn up in consultation with ICT Manager, IT Specialist and/or Legal Services Manager to ensure there is not conflict with existing agreements relating to security and service delivery of software and hardware product used by Municipality. Security controls, service definitions and delivery levels contained in agreements with third parties must monitored by the ICT Manager to ensure they are maintained as specified in the agreements. Services, reports and records provided by third parties must be reviewed and revised, if necessary, at least annually by the Municipality's as owner of the related systems with recommendations from ICT Manager.

Where data is created, changed or possibly deleted on the host systems audits should be carried out as frequently as determined by the Chief Internal Auditor and the ICT Manager. Changes to Services, reports and records provided by third parties must be managed. Proposed changes must be presented to the ICT Steering Committee to determine the impact on all the users at the Municipality. Agreements must be amended before any work is commenced with.

15.4. Manage Database Operations Procedures

The Municipality uses Oracle to manage data base operations. There are standards and procedures developed for database usage to ensure consistency and the effectiveness of the database. Instilled in this process in conjunction with MWEB, the Municipality has standards that cater for the processes of handling specific events such as a disaster recovery plan. The privileges and roles to manage the database are allocated in the following manner:

- Permitting only certain users to access, process, or alter data.
- Applying varying limitations on user access or actions. The limitations placed on (or removed from) users can apply to objects such as schemas, tables, or rows or to resources such as time (CPU, connect, or idle times). Roles are created by users (usually administrators) to group together privileges or other roles. They are a way to facilitate the granting of multiple privileges or roles to users. This is described in the following general categories:
    I. **System privileges.** These privileges allow the grantee to perform standard administrator tasks in the database. Restrict them only to trusted users. "Managing System Privileges" describes system privileges in detail.

II. **User roles**. A role groups several privileges and roles, so that they can be granted to and revoked from users simultaneously.
III. **Object privileges.** Each type of object has privileges associated with it. "Managing Object Privileges" describes how to manage privileges for different types of objects.

15.5. Malicious Code Management Procedures

The malicious code management procedures will ensure that:

- Anti-virus software will be installed on the server and kept up-to-date.
- All servers will sit behind firewalls.
- User access to server desktop environments, where required for remote desktop purposes, will be strictly controlled by the policy in order to block access to system programs, tools, files and processes. User access will have no administrative rights, installation rights or elevated privileges.
- Internet Explorer will only run in Enhanced Security Configuration mode.
- The server will run different anti-virus software to workstations
- New software, portable media and information in electronic format from external sources shall be scanned for malicious program code before being run in the production environment.
- Users must refrain from disabling, halting, freezing or changing the configurations of the anti-virus software installed on their computers.

15.6. Physical Security Procedures

The Municipality has installed and is maintaining servers to provide the platform for all its ICT systems and services. The physical and logical security of these servers is consequently a vital component in guaranteeing confidentiality, integrity and availability of its server.

- All servers will be hosted within dedicated server rooms.
- All server rooms will have secure perimeters.
- All server rooms will have access restricted by Access Control and additionally by barrel-lock keys.
- Access will be limited to members of ICT services engaged in server, network and telecommunications installation and maintenance work.

15.7. Network Security Management Procedures

A range of network controls is necessary to achieve and maintain security in computer networks. Network controllers must implement controls to ensure the security of data in networks, and the protection of connected services from unauthorized access. In particular, the following controls must be enforced:

I. Operational responsibility for networks must be separated from computer operations;
II. Responsibilities and procedures for the management of remote equipment, including equipment in user areas, must be established and communicated;
III. Where necessary, special controls must be established to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems. Special

controls may also be required to maintain the availability of the network services and computers connected; *and*

IV. Management activities should be closely co-ordinated to optimize the service to the business and to ensure that controls are consistently applied across the information processing infrastructure.

15.8. Operating Systems Baseline Procedures

The purpose of the ICT security baseline procedures is to:

- Assess the current security practices of ICT unit within the Municipality.
- Identify tasks for the unit to meet security standards set by the ICT Security Unit
- Implement the capability to monitor security metrics.

The ICT security practice is intended to inform each unit of the necessary actions required to ensure that practical, basic security measures have been implemented that reduce the risk of unauthorised access to ICT resources and data. The baseline requirements are intended to create a minimally acceptable security standard in which all the departments are required to adhere to.

15.9. Security and Training Awareness Procedure

All employees and where relevant, third-party users, should be required to undergo appropriate training and regular updates in organisational policies and procedures in so far as these impact on security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities, particularly where changes have been introduced.

15.10. Administrator / Special Access Procedure

Only employees who have been granted administrator access may make use of privileged access. Administrator and root-level system accounts must be strictly controlled. Administrators are required to log in with their own dedicated user IDs when performing day-to-day operations, and evaluation of administrator privileges should only be used when required. All tasks to be performed by the system administrators are required to be traceable to specific individuals via the use of comprehensive logs or audit trails and unique IDs, and these logs shall be reviewed on a regular basis by the relevant manager or job owner in respect of the operation in question.

15.11. Access Reviews Procedures

All accounts shall be reviewed at least annually by the relevant ICT official to ensure that access and account privileges are commensurate with job functions, need-to-know, and employment status. The ICT official, or any other staff that shall be designated to perform the task, may also conduct periodic reviews for any system connected to the Municipality's network. All guests such VIPs or Dignitaries shall be provided with temporary accounts equivalent to the time period of their stay, more especially those who are not official users of the Municipality. These accounts shall contain an expiration date as per arrangements or whatever the agreement would be, and such accounts must be sponsored by the appropriate authorised member of the administrative entity managing the resource.

15.12. Patch Management Procedures

15.12.1. Term Definition:

- **CERT:** Computer emergency response teams (CERT) - are expert groups that handle computer security incidents
- **Network Devices:** Any physical component that forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc
- **Network Infrastructure:** Includes servers, network devices, and any other back-office equipment.
- **OS:** Operating Systems (OS) - A fix to a known problem with an OS or software program. For the purposes of this document, the term “patch” will include software updates.
- **Patch:** A piece of software designed to fix problems with or update a computer program or its supporting data.
- **Rollback -** an operation which returns the database to some previous state. Rollbacks are important for database integrity, because they mean that the database can be restored to a clean copy even after erroneous operations are performed.
- **Virus:** A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
- **Vulnerabilities -** weaknesses in software that can be exploited by an entity to gain elevated privileges is authorised to have on a computer or system. Not all vulnerabilities have related patches. These situations require workarounds to attempt to mitigate “un-patched” vulnerabilities.
- **WSUS:** A server that enables IT administrators to deploy the latest Microsoft products updates.

15.12.2. Roles and Responsibilities:

System Administrator	➢ Tasked to manage the patching needs for the Microsoft Windows servers on the municipality's network. ➢ Report the patch management status of the municipality on a monthly basis to the Executive Director of Corporate Services using the Patch Management Compliance Form. ➢ Establish and implement a departmental program for patch management on all IT systems.
IT Technicians	➢ Tasked manage the patching needs of all workstations on the network ➢ Monitor patch management on a municipal-wide basis.
Information Security Officers	➢ Responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management. ➢ Ensure that a departmental inventory of hardware and software patch status is developed to maintain and track the status of all patch actions and vulnerability corrections and to provide rapid response to internal or external reporting requirements.
Service Provider (MWEB)	➢ Ensure that security patches/hot fixes are performed in a timely manner as laid out in this policy. ➢ Review current threats and vulnerabilities and to check relevant advisories to monitor any potential threats or vulnerabilities. ➢ Report the patch management status of the municipality on a regular basis to the IT Officer.
Staff and Third Parties	➢ Ensure prudent and responsible use of computing and network resources. ➢ Report any suspected lack of compliance with this policy to the IT Officer. Contrary to this, any failure to do so constitutes a violation of this policy.

15.12.3. Monitoring, Reporting and Enforcement:

The active patching teams as per roles and responsibilities are required to compile and maintain reporting metrics that summarise 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 Information Security and Internal Audit upon request. The onus and the responsibility for continued implementation and enforcement of this policy lies in all employees at Setsoto Local Municipality.

The IT Officer and relevant service provider will monitor and/or subscribe to security mailing lists, review vendor notifications and web sites and research specific public web sites for the release of new patches. Monitoring will include, but not be limited to, the following:

I. Scanning the municipality's' network to identify known vulnerabilities.
II. Monitoring Computer Emergency Readiness Team, CERT, other advisories and websites of all vendors that have hardware or software operating on the municipality's network.
III. Where a vendor has no subscription service available for the notification of patches that are released, the IT Officer and relevant service provider will perform manual monitoring at least monthly.

15.12.4. Implementation:

The patch management procedure shall be implemented to highlight the handling of patch information sources whereby prioritisation on hardware-software compatibility testing requirements, change management, installation, deployment, updates consistency and the monitoring of continuous compliance shall be emphasised. This procedure encompasses the requirements for maintaining up-to-date system security patches on all Setsoto Local Municipality owned and managed workstations and servers.

I. **Workstations** - Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by Setsoto Local Municipality. Any exception to the policy must be clearly defined and documented. The servers will download the patches during the night and upload to workstations during the day. This setup is intended at reducing network bottlenecks.

II. **Servers** – The servers must comply with the minimum baseline requirements. These minimum baseline requirements shall define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the municipality's asset and the data that resides on the system. Any exception to the policy must be clearly defined and documented.

The IT Officer or any other person within the IT Unit whose scope of work shall comprise of the patching management procedures shall;

I. Obtain authorisation for implementing Emergency patches via an emergency change
II. Implement Emergency patches within eight hours of availability. As Emergency patches pose an imminent threat to the network, the implementation may precede testing.
III. Perform testing pre-implementation and document it for auditing and tracking purposes.

IV. Implement High, Medium and Low patches during regularly scheduled maintenance (downtime) windows. Each patch will have an approved change record.
V. Patches will be implemented on all devices according to the timeframes below:

PATCH CRITICALITY	IMPLEMENTATION TIMEFRAMES
Emergency	Within 8 hours of availability
High	Within 30 days of availability
Medium	Within 60 days of availability
Low	Within 90 days of availability

15.12.5. Patch testing Procedures:

All security-related patches must be tested and installed for all hardware, operating systems and software packages as soon as they are released. These patches will be kept current and implemented in a controlled manner. Servers must comply with the minimum baseline requirements to have regular updates of the operating system. Such baseline requirements define the default operating system level, service pack, hotfix, and patch levels required to ensure the security of the Municipality's assets and data. ICT Technicians may need to prioritise the deployment of new patches, performing a risk assessment to determine which systems should be patched first. The following criteria must be followed:

- **Threat:** assess if there is any potential direct danger to information systems (like web servers, email servers and servers with sensitive information).
- **Vulnerability:** assess the absence of or a weakness in a safeguard which could be exploited by an attacker (like flawed software service running on a server or unrestricted modem dial-in access).
- **Criticality:** assess how important or valuable the system is to business operations (like mail servers, database server and network infrastructure).

Exclusions to patches not rolled out due to compatibility issues must be formally documented, and risks which arise from these exclusions must be mitigated through other means. The ICT Manager has the duty and the Internal Auditor may conduct random assessments to ensure compliance with this policy without prior notice, and any system found to be in violation with this policy, shall require immediate corrective actions. Violations shall be noted in the Municipality's issue tracking system and a relevant ICT technician shall be dispatched to remedy the issue at hand. Repeated failures to follow the policy may lead to disciplinary actions been taken against the defaulters.

15.12.6. Windows Server Update Service (WSUS).

The Municipality has set up a WSUS Server (Windows Server Update Services) to handle Patch Management. Therefore, as per procedures set down, WSUS enables administrators to fully manage the distribution of updates that are released through Microsoft Update to computers in the network.

The server provides features that administrators need to manage and distribute updates through a management console. This can be the update source for other WSUS server that acts as an update

source called upstream server. WSUS is operable to be implemented to at at least one WSUS server in the network, thereby connecting to Microsoft Update to get available update information.

15.12.7. WSUS Practical applications.

This update management is the process of controlling the deployment and maintenance of interim software release into the production environment. Among other things, it maintains operational efficiency, overcomes security vulnerabilities, and maintain the stability of the production environment within the Municipality. Core scenarios where WSUS add value to the municipality's business are:

I. Centralised update management.
II. Update management automation

15.13. Firewall Management Procedures

Firewalls are defined as security systems that controls and restrict unauthorised connectivity and network service. They are an important part of the Municipality's information security infrastructure. Most of the network traffic management is outsourced from MWEB. Therefore, the Municipality is currently hosting from an MIG (Managed Internet Gateway) server onsite. It also roles out as a firewall, mitigating against denial of service attacks and any unauthorised access from the external and internal networks.

The following operational procedures will be implemented in managing, modifying and supporting firewall systems at the institution:

- **Firewall host** – this will be provisioned by the authorised ICT infrastructure personnel, vendor or qualified security expert.
- **Responsibilities** – the relevant designated team (ICT Specialist, Network Technician etc) will be responsible for ensuring that all firewall security-related administrative tasks are implemented and maintained.
- **New Servers** – an extensive change management process will be consulted, and an evaluation made that all servers shall use firewall features that use necessary services to authorised networks or hosts.
- **Firewall services** – individual hosting, would use approved local firewall rules as a second layer of protection.

15.14. Mobile Computer Policy

This policy is designed to protect both the confidentiality of any data that may be stored on the mobile computer and the organizational network from being infected by any hostile software when the mobile computer returns. This policy also considers wireless access. However, it covers any computing devices brought into the organization or connected to the organizational network using any connection method. This includes but is not limited to desktop computers, laptops, and palm pilots. Also considered is data and the sensitivity of the data stored and viewed on the mobile computer including:

I. Email.
II. Data the user is working on that is stored locally.

III. Cached data that is stored locally such as cached data from the user's browser. Windows XP allows for cached files to be encrypted using the encrypting file system (EFS).
IV. Data from the internal network that the user may access while the computer is outside the network.
V. Locally stored user names and passwords.

15.14.1. Responsibility.

The user of the mobile computer will accept responsibility for taking reasonable safety precautions with the mobile computer and agrees to adhere to this policy. The computer user will not be allowed to have administrative rights unless granted special exception by the network administrator. The user of the computer agrees not to use the mobile computer for personal business and agrees to abide by the municipal computer usage policy.

15.14.2. Connection Terms.

- Devices connected to the municipal network must be determined to be a benefit to the organization rather than convenience by the designated IT manager.
- All mobile devices owned by the municipality or allowed on the municipal network must be identified by their MAC address to the IT Section before being connected. (Possibly require static IP address)
- The computer device operator must be familiar with the municipality's acceptable use policy.
- Devices not owned by the municipality are subject to a software audit to be sure no software that could threaten the network security is in operation. All computing devices are subject to a software audit at any time.
- Access rights to the municipal network cannot be transferred to another person even if that person is using an allowed computing device

15.14.3. Protecting the Network.

Mobile computers entering the network shall meet the following requirements.

I. If the computer is owned by the Municipality and used regularly by employees, then it shall be checked according to that part of the policy.
II. If the computer is owned by the Municipality and is returning from a period when an employee used it for travel, the following checks shall be performed.

Determine whether the anti-virus program is up to date, has the latest virus definitions, is configured properly, and is running properly. If it fails one of these conditions or has not been scanned for a virus within the last week, a full virus scan must be done before the computer can be used in the building.

- Test the computer and scan for additional malware such as adware or spyware test to determine whether the computer has a worm.
- Test the state of stored sensitive data to be sure it is encrypted.
- Remove any malware on the computer if any was detected. Log information about any malware found. Log any information about data that was not stored properly.

I. If the computer is owned by an outside organization the following must be done.

- The outside organization must agree in writing to allow a malware scan of their computer and agree pay any costs if malware is found on their computer.
- A full virus scan must be done.
- Test the computer and scan for additional malware such as adware or spyware test to determine whether the computer has a worm.
- Remove any malware on the computer if any was detected. Log information about any malware found. The outside organization may be billed for services depending on organizational policy.

16. SERVER ROOM CONTROLS POLICY.

Purpose:

The purpose of the server room policy is to establish standardised physical security requirements for rooms that houses and contains server (Server – defined as a system entity that provides a service in response to requests from other system entities). Therefore, for this purpose, minicomputers and mainframe computers are among the equipment considered as servers.

Scope of Application

This policy applies to all designated staff and service providers of the Municipality with authorised access to ensure that the appropriate security and control measures are in place, and also to verify whether the security and control procedures of the servers and data are stored within acceptable parameters.

The vulnerability of business critical information systems and data they contain within the server rooms make the site a high value asset requiring a high level degree of protection. Therefore, a range of security measures must be put into place to protect employees information and physical assets accessible with the server room. Much of this policy will govern the procedures and the functionalities required from the personnel authorised to access the server room, as well as the types of safety measures that should be implemented and put to place in that regard.

16.1. Server Room Entry System and Access Policy

The server room needs to be optimally located in the building complex. In addition to the size of the rooms, one must consider factors related to cable security, fire resistance, noise, heating, electrical fields, conduit paths, equipment transport, floor loads and any extrinsic general building structures. It is of important that the following are noted in the design of the room: width/depth/height, raised floors, location of equipment racks and room cooling units (including spare capacity), internal conduits, (generic cabling systems and power), control of air currents, lighting, surface treatment of walls, ceilings and floors, access control and fire prevention.

All the staff members and visitors, more especially those authorised to access the server room i.e. employees, contractors, vendors and consultants, should be granted access upon approval or as per arrangement with the person responsible and functioning in that area through the use of a well-documented request for access document, enlisting the reasons for access. Any suspected faults with doors, lights, or any security equipment should be reported to the member of the staff responsible, and a job request shall be created to attend to the issue as soon as possible.

16.2. Fitting out Requirements

All materials to be used in the server room should be non-combustible, self- extinguishing or fire retardant and have the properties of smooth surface finishing and non-dust shedding. Any pipes and ducts not serving the server room should be removed.

- **Walls/Partitions** – In the server room, rigid floor-to-ceiling perimeter walls/partitions having 2-hour fireproof rating should be erected.

- **Partitions inside** server room may be built to the headroom height. Consideration for ample air circulation has to be made. Half-glazed partitions are recommended for partitions inside the room. Double-glassed partitions for noise reduction may be considered for printer area.
- **Wall Finishing** - Internal walls are to be finished smoothly with emulsion paint or vinyl wall papers. Finishing of light colour can enhance the illumination of the server room.
- **Kerb** - Concrete kerb of floor void height is required to be built along perimeter walls of the computer room and around the piping of air-conditioning equipment to prevent water penetration to and from the server room.
- **Thermal Insulator** - Thermal insulator is used on the structural floor and ceiling to prevent heat gain to computer room, especially when bottom discharged type air- conditioners are used. It also helps to save energy and to minimise the running cost of the air-conditioning system. Permanent thermal insulator may be embedded inside the structural floor (sandwich type) during building construction stage or laid on the structural floor (add-on type) for accommodation revised to be computer room. For the latter one, all junctions between the insulator and fixtures are watertight and airtight. Inclinations are required at areas around the floor drains. An alternative is to install the thermal insulator on the structural ceiling of the floor below the computer room.

16.3. Safety Signs and Information:

Server room can be potentially dangerous, therefore, visitor and workers should be cautioned prior access to mitigate against chances of having fatalities, for instance, floor panels and electrical lines may be exposed or lefty open for any operational reasons. Safety signs and information must be posted and placed at the server room's access points together with the general information detaining out the placements and availability of First-aid, emergency contacts and general health and safety issues.

16.4. Contact information:

The following must be visible;

- Emergency and after hours contact details.
- First aid contact information.
- Fire safety.

16.5. Health and Safety Procedures:

The following health and safety procedures must be made addressed;

- **Heavy Lifting** – No one should attempt to lift heavy documents without necessary help.
- **Working at heights** - No one should attempt to lift the equipment in and out of racks without proper assistance, more especially where the height makes the task more dangerous.
- **Lone working** – Anyone working in the server room for prolonged periods must notify other staff, or anyone who is responsible.
- **Lasers** – Equipment that includes lasers such as fibre channel switches, should be clearly identified using proper labelling.
-

16.6. Power Supply

Computer equipment requires a dedicated power source in conjunction with the use of electrical noise protection device or power conditioner to prevent electrical noise disturbance. For maximum reliability, the independent feeder for the computer equipment must not be shared with any other electrical devices.

- **Uninterruptible Power Supply (UPS)** - It employs a means for charging a bank of batteries as a backup for the mains during a short-term power interruption or to allow the computer system to be closed down. Its requirements depend on the computer power loads to be supported, the lead times to start up the backup emergency diesel generator or a tidy close down of the computer system. Using an UPS containing an isolation transformer and a harmonic reduction filter is be the best alternative possible because it may resolve all power line noise problems and provides a continuous power supply during power interruption.
- **Emergency Power Supply** - A generator is to support the UPS in providing emergency power supply to the computer equipment in a prolonged power outage. The need of generator depends on the service requirements of the computer system. However, the generator should also be able to support other essential facilities and equipment such as the air-conditioning system, security and access control system and lighting.
- **Voltage Standard** The nominal voltage for a three-phase and single-phase power supply is ≈380V and 240V respectively. However, some equipment may require different voltage. Detailed permissible tolerance of the voltage requirement can be referred to the hardware manuals or computer vendors.

16.7. Temperature Control

Computer equipment is operated in an environment of controlled temperature and relative humidity. The air-conditioning system in the server room must be able to control the temperature and relative humidity within the specific ranges automatically and independently.

- **Temperature and Relative Humidity Ranges** - The operating ranges of temperature and relative humidity for computer equipment are usually 20°C ± 3°C and 50% ± 10% respectively with the maximum rate of changes at 3°C and 6% per hour.
- **Temperature/Humidity Recorder** - Electrical temperature/humidity recorders are required in the server room to provide 7-day continuous recording of the environmental conditions. They are wall-mounted at the locations near the computer equipment or other appropriate spots and must have visual and/or audible alarms.

16.8. Raised Floors

Raised floors are recommended for server rooms to facilitate the distribution of cooling air, electrical power, telephony/data cables and water for room cooling units. The heights of floors are designed on the basis of the requirements for the supply of air, electrical cables and pipes. The recommended minimum height is 400 mm (the actual height must be calculated on the basis of cooling requirements or the circulation of cooling air. When constructing a raised floor, the sub-floor should be lowered so that the raised floor is at the same height as the floors in adjacent rooms, such as corridors. Ramps for access should be avoided as these hinder the transport of equipment. Raised floors should be designed with the necessary quality to withstand the weight of equipment which is

to be installed or transported. In important ICT rooms the load may approach 1,500 kg/m². Normally, floors in teaching or office buildings are designed for loads of 300 kg/m²

16.9. Fire Prevention, Detection, and Destruction

In order to minimise fire damages to computer equipment, the equipment and furniture used inside the server room should as far as possible, be made of non-combustible material or at least having minimal fire propagation or smoke generating properties.

- **Fire extinguisher systems** will be particularly relevant in cases where passive measures are unsatisfactory, such as in buildings with high fire energy, in buildings with shafts and channels which are difficult to access and in buildings with large, non-sectionalised floor spaces
- **Detector** - A two-stage detection system, consisting of two sets of detectors and alarm signals in cross-zone operation, is required. Detectors should be located at the headroom, inside the ceiling void and floor void of the computer room. Detectors can be smoke detectors or together with heat detectors.
- **Detecting System** - First fire alarm will cut power to air-conditioning system and be transmitted to the building management office and the nearest fire station. Second alarm cuts all power supply to the computer room and the fire suppression system will be triggered off after a pre-set time interval.

16.10. Prevention of Water Leakage

To prevent possible water leakage in the server room it is imperative that the following issues are taken into cognisance:

- Concrete kerb is required along the perimeter of the server room and power conditioner room.
- All unnecessary plumbing is to be removed away from server room.
- Waterproof power connectors are to be used for under floor power connections.
- All ducts, trunks and pipes for cables should be water-tight and be able to stop the water being led by them.
- All under floor fixtures should be away from the floor drains.
- Waterproof treatment is required for internal wall surfaces, concrete ceiling and structural floor.
- Water detection system in the floor void with audible and visual alarm panel showing one or more locations of water threats is required in server room. If the system is not a linear detection type, mimic diagram showing the locations of the water detectors is necessary.

16.11. Surveillance

Closed Circuit Television System (CCTV) is used to monitor the security as well as operating environment of the server room. The monitor unit is capable of programmable switching for selection of pictures for a multi-camera CCTV system. The requirement of the CCTV system depends on the system security level and mode of operation of the computer system.

17. PRIVACY AND DATA PROTECTION POLICY.

Purpose:

The purpose of the privacy and data protection policy is to secure the flow of information through the restricted and controlled use of ICT communicable resources by giving users access to information for which they have been properly authorised to do so based on their designated duties on the Municipality's system. Therefore, privacy and data protection will also encapsulate all the peripherals and devices performing daily functions of keeping and storing data.

Scope of Application:

This policy is applicable in order to safeguard the privacy rights of staff in relation to processing of business and personal data, in both paper, and electronic format. In this process, employees will be permitted to access the data on request, and all users of the Municipality's information computing technology are bound to comply with the policy governing privacy and data protection policy. It is the Municipality's policy to store data on a network drive where it is regularly backed-up and secured. Therefore, users of information are urged to access the type of information and data for which they have been authorised to do so in order to perform their duties on the Municipality's system and network.

Under no circumstances should a user disclose personal and business or any other confidential information accessible to them to persons that are not authorised. Governed by the provisions of the Misuse of Computers Act of 1990, unauthorised access to and/or modification of information and data at the disposal of an unauthorised person shall constitutes a criminal offence, and such action will be considered as a compromise of the information and data at hand, thus would warrant possible legal actions being taken to the wrongful party.

17.1. Personal Data and Data Protection Act of 1998

Data protection is an aspect of safeguarding a person's right to privacy. As enshrined in the constitution's Bill of Rights, the essence of data protection is to give a person a degree of control over his/her information. Therefore, the law considers such competing interests of administering national social programmes, maintaining law and order, and also protecting the rights, freedom and interest of others. The Act stipulates that personal data shall;

- Be obtained and processed fairly and lawfully.
- Be held for specified law purposes.
- Not be used or disclosed in a way that infringes the purpose or renders the purpose incompatible.
- Adequate, relevant and not excessive for the purpose.
- Accurate and up-to-date.
- Not be kept longer than anticipated.
- Available to the date subject.
- Be secured.

18. FIREWALL POLICY.

Purpose:

The purpose of the firewall policy is to set standards and state rules and guidelines for firewalls and their intended roles within the Municipality. To define the roles of individuals authorised to install and manage firewalls such as employees, vendors, contractors, agents etc.

Scope of Application:

This policy applies to the types of firewalls used, enumerating from specific security appliances and/or firewall devices or types of hardware configurations allowed, and also gives emphasis as to the use of auxiliary or add-on components such as content filters, proxies, VPN server software etc.

18.1. Profile Settings

The user can use these policy settings to configure Windows firewall for each kind of network profile.

18.1.1. Domain Profile: Turn on Windows Firewall.

On computers to which this policy is deployed, this policy setting controls Windows Firewall while the computers are connected to domain networks, such as at a workplace.

- **Yes -** enables Windows Firewall on managed computers while they are connected to domain networks.
- **No -** disables Windows Firewall on managed computers while they are connected to domain networks.
- ✓ *Recommended value*: **Yes**

18.1.2. Private Profile: Turn on Windows Firewall.

On computers to which this policy is deployed, this policy setting controls Windows Firewall while the computers are connected to trusted networks, such as a home network.

- **Yes -** enables Windows Firewall on managed computers while they are connected to trusted networks.
- **No -** disables Windows Firewall on managed computers while they are connected to trusted networks.
- ✓ *Recommended value:* **Yes**

18.1.3. Public Profile: Turn on Windows Firewall.

On computers to which this policy is deployed, this policy setting controls Windows Firewall while the computers are connected to untrusted networks at public places, such as at airports or coffee shops.

- **Yes** enables Windows Firewall on managed computers while they are connected to untrusted networks.
- **No** disables Windows Firewall on managed computers while they are connected to untrusted networks.
- ✓ *Recommended value*: **Yes**

19. E-MAIL / INTERNET POLICY.

Purpose:

The purpose of the email / internet policy is to govern, control and assist in the use of electronic communications through electronic mail system and Internet.

Scope of Application:

This policy is applicable in order to raise awareness to the users as to the care and caution required when utilising the content, giving them a light as to the consequences and actions taken if the provisions are not adhered to. Where technology allows, the policy will be enforced automatically, for instance, Anti-Virus and Internet Proxies can filter and restrict the content been accessed. Management reports will also highlight possible violations, and this might call for further investigation to identify the actual nature of the violation in question. Users will also be encouraged to report any irregularities as evidenced within their respective work stations, or having suspected any misuse of the internet and emailing facilities.

Internet and e-mail usage play a very pivotal role in the execution and development of services and the interaction between employees within the Municipality, in and around, taking into cognisance the stakeholders as well as the different facets within the spheres of government. Individuals or staff endures the privilege to use these facilities in an effort to execute their duties within the best possible time span. Therefore, it remains the Municipality's prerogative to ensure that all authorised users appreciate that the access to these facilities is for the purposes of increased productivity and not for private activities.

19.1. E-MAIL.

Electronic mail (e-mail) is an official method of communication in the Municipality, delivering information in a convenient, timely, cost effective, and environmentally sensitive manner. It is a policy of the Municipality that;

- All relevant personnel have access to email facilities.
- The Municipality may send official communications via e-mail and electronic mailing lists.

19.1.1. Use and Responsibility:

The Municipality's email system is solely provided for official duties. It regards it as a critical business tool and therefore, inappropriate use can expose the institution and the user to significant liability. Copyright or trademark infringement, misuse of confidential information, defamation and inaccurate statements are among some of the liabilities which could arise. The e-mail system cost the Municipality valuable resources such as time and money, therefore, it must be utilised with care equivalently in the way other facilities are handled such as cars, telephones etc. The Municipality must strongly restrict the access to internet through the following ways:

- Grant access to the management and staff that is authorised like personnel in the Debt Collections and Revenue Unit, Policy Researchers, Corporate Services Department, Supervisors and ICT personnel. Also access can be granted as per formal request and

approval pending application by the relevant line Managers or Heads of Department in respect of the employees who shall so deemed not to have had an access before.

- Users must ensure that their access to the facility and content is kept and remains official and at all times avert from using profanity, obscene, racist, defamatory, abusive or threatening, discriminatory or otherwise biased remarks and/or content, lies to discredit the Municipality or any other persons who shall so deemed to be acting as it's representative.

19.1.2. Content:

E-mail messages must be treated like any other formal written communication. Improper statements on an e-mail can give rise to personal liability for the Municipality, and in some other cases, this could constitute a serious disciplinary matter. E-mails that embarrass, misrepresent or even convey an unjust or unfavourable impression of the Municipality or its business affairs, employees, suppliers, customers or even its competitors are not permitted.

Users are advised not to create or forward electronic messages that are defamatory, because defamatory messages whether internal or external can constitute a published libel and are actionable. These includes messages that may be intimidating, hostile, offensive based on sex, race, colour, religion, ethnicity, sexual orientation or disability. E-mail messages, regardless of their confidentiality or damaging content, may have to be disclosed in the court proceedings. It is however, not permissible to subject another employee to public humiliation or ridicule.

19.1.3. Actions Prohibited in Using e-mail Systems:

The following actions are prohibited when employees are using the Municipality's email system:

- Distribution, forwarding and/or advancing and promoting any act that is sexual, pornographic, biased, offensive or violent to disgust or viewed as inappropriate or illegal content.
- Sending emails that contain usernames and passwords to person not on the network or not members of the network, especially if those credential grants the person in question access to the network, when the proper procedures to allow such action have not been followed.
- All the employees are urged to keep email message to a maximum of 10 MB or below (including the attachments). Over-sending of private emails.
- Users must keep their usage of private emails to the minimum, as this will be monitored by the relevant government network monitoring software as prescribed by the Intelligence Act.

19.1.4. Privacy:

E-mail messages to or from users cannot be deemed to be private or confidential. Although it may not be a policy to routinely examine and verify the validity or content of individual emails, the Municipality reserves the right to monitor messages, at any given time, for specific instances in which there is good cause (fulfilling government obligation, detect employees' wrong doing, protect the rights or property of the Municipality as well as the ICT system security to comply with legal processes) for such monitoring or some legal obligation to do so.

Therefore, messages sent or received may be copied and disclosed by the Municipality for lawful purposes without prior notice. It is thus, not permissible to access or send e-mail from another

employee's personal account directly or indirectly, unless one has that person's prior written approval.

19.1.5. Disclaimer Clause:

This message shall be displayed at the end of each and every e-mail. It creates an obligation for the parties in communication to observe the rules governing the e-mail messages as per the Municipality's policy and the manner in which it must be handled.

This message contains information which is confidential, private or privileged in nature and subject to legal privilege. If you are not the intended recipient, you are prohibited from pursuing, disseminating, altering, distributing, forwarding, storing or copying this message (or part thereof) or file (or part thereof) which is attached to this message and any action in reliance on the contents of this e-mail or its attachments is prohibited. If you have received this message in error, please notify the sender by e-mail, facsimile or telephone and thereafter return, delete and/or destroy the original message from your system. The Disclaimer forms part of the content of this email in terms of section 11 of the Electronic Communications and Transactions Act, 25 of 2002., and will therefore, not be held liable for any personal mail and/or opinions expressed herein.

19.1.6. Instant Messaging:

Instant messaging is free, fast, real-time, and powerful. However, instant messaging also carries risk such as the lack of encryption, logging of chat conversations without the user's knowledge and virus risk. Due to these risks, IT office does not currently allow the use of instant messaging for the communication of sensitive or proprietary Setsoto Municipality information.

19.2. INTERNET

The laws regulating diverse subject such as intellectual property, fraud, defamation, pornography, insurance, banking, financial services as well as tax applies equally to online access and activities. Documents which are defamatory, hostile, and /or offensive on the basis of sex, race, colour religion, ethnicity, sexual orientation and even disability, must not be published on the web. The Municipality has a prerogative to allow certain users to access social websites as part of their duty to promote it's work.

Such users will also have express permission in the form of a submission signed by the respective Director in consultation with the ICT Manager. The access request must clearly articulate and give a clear motivation as their job functions indicating the need to access the sites. Employee are by all means regarded to be promoting the business of the Municipality, therefore, is it of utmost importance that such employees ensure that the responsibility in the usage of internet in a manner that is effective, ethical and lawful by;

- Using web browsers to obtain business information from commercial a websites.
- Accessing databases for information as required.
- Using email as a tool for performing assigned duties.

The Municipality promotes the acceptable use policy as enshrined in the provisions of the Constitution of the Republic of South Africa, Act 108 of 1996. Therefore, on this basis, it is

reasonable that the Municipality expects employees to have a good awareness and to be able to exercise good judgement, if in doubt; they may contact the relevant ICT office.

19.2.1. User and Responsibilities:

Employees must ensure that all communication is for professional reasons and that it does not interfere with their productivity at work. They should be responsible for the content of all text, audio and/or images that are placed or sent over the internet. Employees shall not under any circumstances transmit copyrighted material without permission. They must know and abide by all applicable policies dealing with security and confidentiality of the municipal records. They must always run a virus scan on any file received through the internet.

19.2.2. Termination of Internet Access: Non-Compliance

Internet access can be terminated upon abuse, change in nature of work by the employee or any other reason necessitating such action. Termination of internet access shall be communicated in writing to the employee concerned via his/her line manager, with reason for such termination.

19.2.3. Private Use

The Municipality shall provide computing facilities to qualifying employees. It is therefore, required of any employee to adhere and work responsibly provided there is no conflict of interests with the Municipality. The institution shall not accept liability for any personal loss or damage incurred through using the Municipality's computing facilities for private use. Should these arise, the violating of Municipality's resources constitutes misconduct subject to disciplinary action in line with its human resources policies and code of conduct for employees. These are:

- Knowingly gaining unauthorised access to a computer system or database.
- Falsely obtaining electronic services or data without payment of required charges.
- Intentionally intercepting electronic information
- Obtaining, altering or destroying others' electronic information.

19.2.4. Disciplinary Action

The Municipality wishes to promote the highest standards of discipline in relation to acceptable usage of its ICT resources. Consequently, it expects and supports the integrity of its employees. In exceptional circumstances, where there are reasonable and justifiable grounds to suspect that the employee has committed an offence, necessary internal procedures will be followed to discipline such an employee.

Illegal or Prohibited Actions Constituting Misconduct in the use of Internet:

The following actions are deemed illegal and are therefore prohibited:

- Visiting pornographic sites.
- Harassment through emails.
- Obscene racist jokes or remarks.
- Downloading and installing unlicensed products.
- Violation of the Municipality policy and pursuing acts that could be regarded as media counterfeiting or illegitimate distribution of copied software.

- Use of the Municipality computing facilities in order to bring the Municipality into disrepute.
- Deliberate introduction of viruses into the system.

20. BACK-UP AND RECOVERY POLICY

Purpose:

The purpose of the back-up policy is to standardise the procedures by which the Municipality's exercises appropriate back up procedures, ensuring that both data and software are regularly backed up to mitigate contently against the loss of essential information.

Scope of Application:

This policy is applicable in order to provide for the retention period of information contained within the system level backups designed for recoverability, and to provide a point-in-time snapshot of information as it exists on the centrally hosted system during the time period as defined by the backup policy.

Handling of Data and Longevity of Back - Up

The Municipality understands the importance of regular backups to the continued efficient running and continuity of the business. To this end, procedures and systems have been put in place to ensure regular backups are taken from all the departments to ensure that their relevant data is backed-up. These backups are stored in a resource server located and hosted by MWEB separate from the main server system to protect against fire or other hazards.

The backups are carried out automatically at set intervals and information is only accessible by the network systems personnel for verification and restoration. The backup logs are then checked weekly to ensure backups have processed correctly and this information is logged by the network systems personnel. The backup method carried out and the backup intervals mean that no restoration tests are required.

This policy applies to all data owned by the Municipality that is critical to the successful operation of the business. Not covered in this document are any guidelines or policies relating to Disaster Recovery.

Definitions

- Backup - The saving of files onto magnetic tape or other offline mass storage media or online storage for the purpose of preventing loss of data in the event of equipment failure or destruction.
- Archive - The saving of old or unused files onto magnetic tape or other offline mass storage or online storage media for a specified period per set archiving standard.
- Restore - The process of bringing data back from the storage media back into the live system or test system.

- Disaster Recovery – The short term provisioning of systems and data to aid in business continuity in the event of a major equipment failure or natural or human induced disaster.
- Emergency Restore – Data loss that will result in direct or indirect financial, reputational damage is deemed grounds to implement an Emergency Restore.
- Power User – High level users (CFO, Accounting Officer, etc and others as identified by the IT Manager)
- Selection List – Data deemed essential to the business as defined by the organisation

20.1. Frequency (Servers)

Full backups are performed:

- Initial take on of any backup frequency, daily, monthly, yearly backup before incremental begins.
- Monthly – On the same evening that month end procedures are run, after 10:00, to complete before 7:00
- Yearly – On the same evening that year end procedures are run, after 10:00, to complete before 7:00

Incremental backups are performed:

- Daily – Monday, Tuesday, Wednesday, Thursday & Friday after 10:00, to complete before 7:00 and on any other frequency provided the data retention period has been adhered to. Reporting & Monitoring:
- Daily – Monitoring of backup success/failure
- Monthly – Send report to the chairperson of the ICT Steering committee or person accountable for backups in the organisation

20.2. Exceptions

Backup exceptions include:

- Failure to start
- Failure to complete before 7:00
- Complete with warnings
- Complete with errors

Should any of the above events occur, ICT/Business must ensure the following actions must be implemented:

- Log the incident in the IT incident tracking system
- Advise the affected managers/system owners
- Manually start a new backup (provided systems performance is not affected to the extent that users and/or clients cannot operate)
- Perform continuous troubleshooting to ensure backup success
- Ensure exception is documented with remedial action taken to resolve exception and inform affected manager/system owner
- Follow up on each incident logged to ensure no exception is repeated

20.3. Retention & Archiving

Data retention must is and should be designed according to regulatory requirements.

Backed up data must reside offsite. Should the live/primary site be struck by disaster, backed up data must remain available and accessible. Therefore:

If the backup technology in place relies on tapes or other onsite storage media, the media should reside:

- ✓ At the bank that the organisation has an account with,
- ✓ At An offsite office/regional office If no bank exist,
- ✓ In a fireproof & waterproof safe

If the backup technology in place is an online backup system:

- The destination data centre should be more than 5km away from the primary site
- The destination data centre must be appropriately secured, i.e. only authorised persons may gain access, appropriate environmental controls

20.4. Retention & RPO:

- Onsite Data Retention Period: 2 Roll-ups storage on the Primary Platform
- Offsite Data Retention Period: 2 Roll-ups storage on the Mirror Platform
- Data Recovery Point: RPO – 24 hours, backups run on a daily basis

20.5. Responsibility

While the IT department manager remains accountable, this manager may delegate a member of the IT department to perform:

- Regular backups monitoring and reporting.
- The delegated person will use the procedure for testing backups and test the ability to restore data.
- If used backup method is tape, the delegated official will also be responsible for external drive rotation, labeling and transporting from onsite to offsite
- If used backup method is online, the delegated official will be responsible for ensuring that backups are being monitored.

20.6. Selection List

Financial Management Data

- ➢ Current live database
- ➢ Current live data
- ➢ Server system state

Human Resources & Payroll Data

- ➢ Employee Files (current and historical)
- ➢ Payroll databases (current and historical)
- ➢ Server system state

Domain Controller

- Server system state

File Server

- Server system state
- Data

Application Server

- Application(s) current live database
- Application(s) current live data

20.7. Default exclusions\filters unless specified:

- Personal archive mail files such as (but not limited to) .pst, .ost
- Video files such as (but not limited to) .wmv, . avi, .mov,.mkv, .mp4
- Audio files such as (but not limited to) .mp3, .wav, .ogg, .wma
- Images such as (but not limited to) .jpg, .tiff, .jpeg, .bmp
- Executable files such as (but not limited to) .exe, .bat, .com, .msi, .pkg

20.8. Restoration & Testing

Users that need files restored must submit a request to the help desk.

- The file restoration requisition should be completed and should include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was destroyed, this process has to be authorised by the appropriate supervisor of the requesting employee.

System Restore

- Should there be a system failure where an emergency restore is required, the system administrator may restore the necessary data and t hen later document the restore and test thereof and have the documentation approved by the supervisor of the affected section.
- All application data and User Data will be restored according to the restore procedure to test and ensure that the backed up data is still in working condition and that backup was 100% successful.

Testing

- The ability to restore data from backups shall be tested as per the application/system set rules. All tests conducted will be logged on the test schedule document.
- Restore tests are to be performed as per agreed schedule of service and the identified personnel as per schedule of service is to sign off on success or failure thereof.

In the event of test failure, the failure must be logged in the appropriate incident tracking system and Root Cause Analysis provided. This RCA will be used to prevent repeat of failure. Once the incident is resolved, the restore test must be run to succes sful completion.

21. ICT SERVICE LEVEL AGREEMENT MANAGEMENT POLICY.

Purpose:

The purpose of the ICT Service Level Agreement is to ensure efficiency and integrity of Systems and the effectiveness of the ICT Unit in responding to requests, queries and other systems needs of users. Service Level Agreements (SLA) will be entered into between each User Department, the Office of the Municipal Manager (representing all Directors) and the Office of the Executive Mayor (representing the Members of the Mayoral Committee).

Scope of Application:

This policy is applicable to the relationship between the Municipality and the external service providers (vendors and consultants), defining the nature in which contractual agreements and service level agreements will be managed and rolled out to cover the prerequisites arising from the obligations binding on both parties. A separate SLA between the ICT Unit (Service Provider) and each department (client) must be drawn up and signed by the Municipal Manager represented by ICT Manager, the Director of each Department. The SLA must:

- Clearly indicate the services provided by the SP.
- Provide for different service levels.
- Clearly indicate the priorities attached to the service levels.
- Clearly indicate the type of circumstances where the service levels and priorities in the SLA may be overridden.

21.1. Time frame for Revisiting the SLA

The SLA must be revised annually to ensure that environmental and / or systems changes are taken into account and adjusted accordingly. Should an SLA be changed, the new SLA must be signed as in paragraph 1 above, and replace the existing one. The Municipality shall ensure that sufficient competent staff is appointed to make the SLA viable.

21.2. Security Requirements and Outsourcing of Contracts

This emphasises the security requirements of the Municipality with regard to any outsourcing of the management and control of all or some of its information systems, networks and/or desk top environments, and the manner in which this must be reduced to writing in a contract agreed between the parties. The following shall be pointed out in a contract:

- How the legal requirements are to be met such as data protection legislation,
- What arrangements will be put in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities,
- How the integrity and confidentiality of the Municipality's business assets are to be maintained and tested,
- What physical and logical controls will be used to restrict and limit the access to the Municipality's sensitive business information to authorized users,
- How the availability of services is to be maintained in the event of a disaster;
- What levels of physical security are to be provided for outsourced equipment?

22. REVIEWS OF SECURITY POLICY AND TECHNICAL COMPLIANCE

The security of information systems must be reviewed regularly. Such reviews should be performed against the appropriate security policies and the infrastructural platforms and information systems should be audited for compliance with security implementation standards.

22.1 Compliance with Security Policy

Management must ensure that all security procedures within their respective areas of responsibility are followed correctly. In addition, all areas within the Municipality should be considered for regular review to ensure compliance with security policies and standards. These should include the following:

(a) Information systems;
(b) Systems providers;
(c) Owners of information and assets;
(d) Users; *and*
(e) Management.

Owners of information systems should support regular reviews of the compliance of their systems with the appropriate security policies, standards and any other security requirements, including monitoring of system usage.

22.2. Technical Compliance Checking

Information systems should be checked regularly for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking usually requires specialist technical assistance and should be performed manually (supported by appropriate software tools, if necessary) by an experienced system engineer or by an automated software package that generates a technical report for subsequent interpretation by a technical specialist. Any technical compliance check should only be carried out by, or under the direct supervision of, competent, authorized persons.

22.3. Systems Audit Considerations

Controls are necessary to safeguard operational systems and audit tools during system audits. Protection is also necessary to safeguard the integrity and prevent misuse of audit tools.

22.3.1. Systems Audit Controls:

Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimize the risk of disruptions to business processes. The following should be observed:

- Audit requirements should be agreed with management;
- The scope of the checks should be agreed and controlled;
- The checks must be limited – as far as possible - to read-only access to software and data;
- Access other than read-only should only be allowed for isolated copies of system files, which should be erased once the audit is completed;

- Municipal Information Systems (MIS) resources for performing the checks should be explicitly identified and made available;
- Requirements for special or additional processing should be identified and agreed;
- All access should be monitored and logged to produce a reference trail; and
- All procedures, requirements and responsibilities should be documented**.**

22.3.2. Protection of System Audit Tools:

Access to system audit tools, i.e. software or data files, should be protected to prevent any possible misuse or compromise. Such tools should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

23. POLICY IMPLEMENTATION

This policy will be implemented once it has been approved by the Council as part of the Municipality's policies.

23.1. Policy Availability

This policy shall be freely available in hard copy, electronically and on the Municipality's intranet site.

23.2. Short Title

This policy shall be referred to as the Setsoto Local Municipality's Information and Communication Technology Policy

23.3. Enquiries

Any inquiries with regard to this policy shall be directed to the Manager: ICT

24. Conclusion

The network and Information Technology as a whole is very important to any organisation and abuse of such services may lead to large bills in support and repairs as well as security breaches in some cases. Unfortunately strict action is important and cannot be ignored and users should be made aware of such actions. There cannot be a scenario where freedom reigns on the network and users have free access to do as they please. It is very important to control and properly implement the policy to act as a tool to ensure such control and to ensure that the relevant performance and security levels are reached on the network and with Information Technology as a whole.

The policy on ensures the protection of the government employee and the interests of the government, locally, provincially and nationally. Without such control measures the transparency policy is not adhered to and a secure network becomes insecure, unstable and very expensive to maintain.

25. GLOSSARY, DEFINITIONS AND ABBREVIATIONS:

Municipality	Refers to Setsoto Local Municipality.
ICT	Refers to Information Communications Technology.
Attachments	Files created in other applications (such as Ms-Word, MS-Excel) or pictures.
ADSL	Asymmetric Digital Subscriber Line is a data communications technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide.
Default Gateway	The routing device used to forward all traffic that is not addressed to a station within the local subnet.
CCTV	Closed Circuit Television.
Directory	An entity in a file system, which contains a group of files and/or other directories.
Domain	A logical group of computers running versions of the Microsoft Windows operating system that share a central directory database.
DHCP	Dynamic Host Configuration Protocol- This protocol allows a computer (or many computers or devices on your network) to be automatically assigned an IP address from a DHCP server.
DNS	Domain Name System – This system allows internet host computers to have a domain name and one or more IP addresses. A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a User enters a domain name into a web browser they are sent the proper IP address for that domains host. Most home Users use their ISP's DNS server
Domain Controllers	A server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server domain
E-mail	An electronically transmitted message, along with attachments and any information appended by the e-mail system.
E-mail System	Computer hardware and software system that allows personal computer Users to send, receive and store messages, documents and files with other individuals or groups of people over an internal network or the Internet.
Encryption	A means of coding messages so they appear to be random characters. Encryption has two benefits. First, it prevents disclosure of sensitive information to unauthorized third-parties. Second, encryption allows for “authentication” of the information sent.
Firewalls	A firewall determines which information passes in or out of a network. NAT can create a firewall by hiding networks IP addresses from the internet. A firewall prevents anyone outside of your network from accessing your computer.

Hacking	The unauthorized attempt or entry into any other computer system.
Hardware	A general term that refers to the physical artefacts of a technology.
HOD	Head of Department.
Internet	A worldwide computer network through which you can send a letter, chat to people electronically or search for information on almost any subject you can think of. Quite simply it is a "network of computer networks".
Internet Browser	An application that displays HTML and other information found on the Internet. Internet Explorer is an example of an Internet Browser. This type of client software accesses the World Wide Web and Gopher services and lets you drift from link to link without having to have a purposeful search.
IP Address	Internet Protocol address - Used to identify a computer connected on the network. It consists of four sets of numbers separated by a full stop that identifies a unique network computer host or client. It allows data messages intended for that computer to be delivered to the correct destination.
ISP	Internet Service Provider - An ISP is a business that allows individuals or businesses to connect to the internet. Users log on to the internet using an account with an ISP.
LAN	Local area network is a computer network covering a small physical area (Within 1 KM)
Network Drive	A hard-Disk or shared space that is normally shared among several Users over the network.
Public Record	Includes all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body. Records which contain names or other personally identifying details regarding the Users of public, private, school college, university etc.
Public Resource	Includes not only Municipality equipment, hardware, software or tangible articles, but also the employee's time expended while on duty with the Municipality.
Risk	Those factors that could affect confidentiality, availability, and integrity of the Municipality's key information assets and systems. The Municipality is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.
Server	Any combination of hardware or software designed to provide services to clients.
SLA	Service Level Agreement - is a part of a where a service is formally defined. Particular aspects of the service scope, quality, responsibilities are agreed between the service provider and the service user.

Shareware	Software that is distributed free on a "trial basis" with the understanding that the User my need to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date. Other shareware is offered with certain capabilities disabled as an enticement to buy the complete version of the program.
Software	A general term used to describe a collection of computer programs, procedures and documentation that perform some task on a computer system.
Switches	A computer networking device that connects network segments.
Subnet Mask	A subnet mask is a set of four numbers similar to (and used in conjunction with) an IP address. It is used to create IP address numbers used only within a particular network.
Routers	A networking device whose software and hardware are usually tailored to the tasks of routing and forwarding information.
Third Party	Any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. A third-party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and trainers.
Users	Any individual who has access to our information systems for the purpose of performing work. Users consist of, but are not limited to: employees, Councillors, third parties etc.
UPS	Uninterruptible Power Supply.
World Wide Web	A hypertext-based distributed information system for linking databases, servers, and pages of information available across the Internet.
WAN	Wide Area Network - A system of LAN's connected together. A network that connects computers located in separate locations. The internet is a Wide Area Network.
3G	Mobile phone communication standard.

26. SOURCES:

Tipton, Harold F.; Micki Krause; *Information Security Management Handbook, 6th Edition*, 2007

ISACA, COBIT 5, USA, 2012, www.isaca.org/cobit5

Swanson, Marianne; Barbara Guttman; SP 80014, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996, http://csrc.nist.gov/publications/nistpubs/80014/80014.pdf

Bowen, Pauline; Jan Hash; SP 800100, *Information Security Handbook: A Guide for Managers*, October 2006, http://csrc.nist.gov/publications/nistpubs/800100/SP800100Mar072007.pdf

http://www.comptechdoc.org/independent/security/policies/mobile-computer-policy.html

Douglas E Comer, *Computer Networks and Internets with Internet Applications. 3rd Edition*. Prentice Hall 2001

Microsoft Windows 2003 Server administrators Pocket Consultant 2nd Edition
(William R. Stanek) ISBN 0-7356-2245-6

Microsoft Windows Security Resource Kit 2nd Edition
(Brian Komar) ISBN 0-7356-2174-8

Microsoft Internet Security & Acceleration Server 2004
(Bud Ratliff & Jason Ballard) ISBN 0-7356-2188-8
www.computer-policy.com

www.attackprevention.com

SUNY College at Oneonta Information Technology Program
(http://www.oneonta.edu/technology/security/security_program.asp)

http://csrc.nist.gov/groups/SMA/fasp/documents/policy_procedure/Patch-Management-and-SystemUpdates.pdf

27. ACCEPTANCE OF POLICY

All employees that are granted the use of I.T. equipment will be provided with a written copy of this policy.

Employees must sign the statement below as acceptance of this policy.

I, _____ ID. No. _____

(Full name printed)

Employee No. _____ hereby accepts the terms and conditions of the Setsoto Local Municipality's Information Technology Security Policy. I understand that disciplinary action will be instituted against me should I breach any clause of the said policy.

Signed at Setsoto Local Municipality on this _____ day of _____20____.

_____

Signature

As witnesses: 1._____

2._____