Maruleng Local Municipality

Information Technology

Policies and Procedures

TABLE OF CONTENTS

VERSION CONTROL

Version	Date	Author(s)	Details
1.0	23/03/2012	Masilo Modiba	First Draft
1.1	08/10/2021	Tshepo Manyama	First Revision

REFERENCES

This policy document shall be read in conjunction with the following Acts and Standards.

- COBIT Audit Framework
- Copyright Act 98 of 1978
- Electronic Communication Transaction Act
- Fire brigade Act 99 of 1987
- Government Gazette, 26 November 2013. Act No. 4 of 2013
- Information Security Forum (Code of good practice for Information Security)
- Information Security Policy: Securing Information in the digital Age (Draft)
- International Standard for Risk Assessment
- ISO 17799
- Limpopo Information Security Policy
- Local Government Municipal Structure 117 Act 0f 1998
- Local Government Municipal Systems Act 32 of 2000
- Maruleng Local Municipality Supply Chain Management Policy
- Minimum Information Security Standards
- Minimum Information Security Standards (MISS). (The purpose of the MISS is to establish policy frameworks for general guidance of Information Technology practices to ensure that IT as strategic resource is utilized fully and cost effectively
- Municipal Finance Management Act 1 of 2004
- Protection of Information Act
- The Constitution of the SA, Act 108 of 1996
- The National Archives Act 43 of 1996
- The promotion of Access to Information Act
- The protection of Information 84 Act of 1982
- The State Information Technology Agency (SITA) Act, as amended.

DEFINITIONS OF ABBREVIATIONS AND TERMS

Access Control	Mechanisms and policies that restrict access to resources.
Accountability	Ensuring that the actions of an entity or individual may be traced uniquely to that entity or individual, who may then be held responsible for that action.
AC	Alternating Current, an electrical current that frequently reverses direction, supplied from mains.
Authentication	Authentication is the act of verifying the identity of a user or process. It is the process of determining whether someone or something is, in fact, who or what it is declared to be. It answers the question: "*Are you who you say you are?*"
Authorization	Authorization is the function of specifying access rights to information technology resources
BIA	Business Impact Analysis, the process that identifies critical business functions, set priorities and determines the impact on the organization if those functions are not performed for a specified period of time.
Biometrics	Process by which a person's unique physical and other traits are detected and recorded by an electronic device or system as a means of confirming identity.
CA	Capability Assessment, ITO assessment of the estimated recovery time of critical services.
CAB	Change Advisory Board
Cascading	Cascading is the term often given to the movement of PCs within an organization
CCTV	Closed Circuit Television is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.
CD	Compact Disk
CFO	Chief Financial Officer
CIO	Chief Information Officer
CMB	Change Management Board
COBIT	Control Objectives for Information and related Technology, an industry framework that defines generic processes for management of Information Technology.
CoGHSTA	Limpopo Provincial Department of Corporative Governance, Humans Settlements and Traditional Affairs.
COGTA	National Department of Corporative Governance and Tradition Affairs
Computer virus	A computer program or script that interferes with, or damages the normal operation of a computer or any installed software. Virus programs are designed to infect other computers by hiding within e-mails or executable programs.
Copyright	Copyright is designed primarily to protect an artist, publisher, or other owner against any unauthorized copying of his works, by reproducing the work in any material form, publishing it, performing it in public, filming it, broadcasting it, causing it to be distributed to subscribers, or making any adaptation of the work. A copyright supplies a copyright holder with a kind of monopoly over the created material, which assures him of both control over its use and the pecuniary benefits derived from it.
Data Centre	Facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes

	redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.
Data Subject	The person to whom personal information relates to.
Download	Acquiring (getting) a file/data from internet.
Disaster Recovery Team	A temporary team assembled during an Emergency Management situation/outage. This team is led by the team leader / incident coordinator.
DRP	Disaster Requirement Planning
EMS	A network management system that manages one or more network elements of a specific type, e.g., modems or multiplexers, and manufacturer.
EMT	Emergency Management Team – an MLM cross-functional response team that manages potential/actual large-scale disasters/outages.
EULA	End-User License Agreement, in the proprietary software industry, an end-user license agreement or software license agreement is the contract between the licensor and purchaser, establishing the purchaser's right to use the software.
Fire Extinguisher	An active fire protection device used to extinguish or control small fires, often in emergency situations.
FTP	File Transfer Protocol, used for transferring data/files on the internet.
GIS	Geographical Information Systems.
GIS	Geographical Information Systems.
Grandfather-father-son	A common rotation scheme for backup media, in which there are three or more backup cycles, such as daily, weekly and monthly.
Hyperlink	Automatic link to a URL.
IARF	Information Asset Release Form.
IAUU	Internet Acceptable Use Undertaking.
ICT	Information & Communication Technology.
Identification	Identification is the method used to distinguish one user from all others. Identification techniques provide a means of providing authorized entry to the Municipality's resources such as workstations, networks and applications. Identification is closely linked to authentication.
Information Officer	means the person who is responsible for ensuring MLM compliance with POPI Act.
Internet	The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite.
Internet Proxy	A server (a computer system or an application) that acts as an intermediary for requests from client's computers seeking resources from other servers.
In-house	Conducting an activity or operation within a company/municipality, instead of relying on outsourcing.
IP	Intellectual Property.
IP	Internet Protocol, the principal communications protocol used for relaying datagrams (also known as network packets) across an internetwork using the Internet Protocol Suite.
ISP	Internet Service Provider, an organization that provides access to the Internet.
IT	Information Technology, a branch of knowledge concerned with the development, management, and use of computer-based information systems.

ITARF	Information Technology Asset Release Form.
ITIL	Information Technology Infrastructure Library, a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business(municipality).
ITO	Information Technology Office, managed by the IT Officers.
MLM	Maruleng Local Municipality.
MM	Municipal Manager.
Municipality	Maruleng Local Municipality.
P2P	Computing or networking distributed application architecture that partitions tasks or workloads among peers.
PC	Personal Computer.
Personal Account	An account created on the computer for individual User for official usage.
Personal Computer	Computer Equipment being a Desktop or Laptop/Notebook assigned by **MLM** to personnel for business activities and official use.
Personal Information	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person
Personnel	Includes employees/staff/officials employed permanently and temporarily as well as supplied by labour brokers or service-providers
POPIA	Protection of Personal Information Act 4 of 2013.
Prescripts	Regulations, instructions and directions.
Processing	Any operation or activity or any set of operations, whether by automatic means
Raised Floor	Types of floor that provide an elevated structural floor above a solid substrate (often a concrete slab) to create a hidden void for the passage of mechanical and electrical services.
Record	means any recorded information regardless of form or medium.
Removable storage device	A removable disk on which data may be stored. Usually refers to the 3½-inch diskette. For the purpose of this policy this term includes any removable storage device fitted to a personal computer.
Responsible Party	Public or private body or any other person which, alone or in conjunction with others determines the purpose of and means for processing personal information.
ROI	Return on Investment, used to evaluate the efficiency of an investment in finance and economics.
RPO	Recovery Point Objective, it represents the maximum amount of data loss an institution can tolerate for a given application in the event of a disaster.
RSA	Republic of South Africa
RTO	Recovery Time Objective, it represents the maximum amount of time an institution can tolerate the loss of an application or, conversely, how quickly an application must be restored to working order in the event of a disaster.
Senior Managers	Municipal Manager and managers referred to in section 56 of the Municipal Systems Act or chief executive officer of the municipal entity and managers directly accountable to him.
SCM	Supply Chain Management, the management of a network of interconnected businesses involved in the provision of product and service packages required by the end customers in a supply chain.
SITA	State Information Technology Agency, established in terms of the SITA Act, No. 88 of 1998 as amended.

SLA	Service Level Agreement, a contractual agreement on the level of service to be provided by a service provider to a customer, commonly used in computer-related services.
SSH	Secure Shell, a network protocol for secure data communication and remote command execution.
SMS	Short Messaging Service, is a text messaging service component of phone, web, or mobile communication systems.
SNMP	Simple Network Management Protocol, an Internet-standard protocol for managing devices on IP networks.
Tailgating	Entering an area without authorization verification by following someone who has access.
TCO	Total Cost of Ownership, a financial estimate whose purpose is to help consumers and enterprise managers determine direct and indirect costs of a product or system.
UID	Unique identifier for a specific User of a computer system or a code identifying each user on a Unix and Unix-like systems.
UPS	An electrical apparatus that provides emergency power to a load when the input power source, typically mains power, fails.
URL	Uniform Resource Locator, the address of a specific website.
VPN	Virtual Private Network, a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible.
User(s)	Authorized individual(s), making use of the Municipality IT Infrastructure.
WWW	World Wide Web, a system of interlinked hypertext documents accessed via the Internet.

1. PREAMBLE

Like any other municipalities, MLM also rely on computer-based systems and data management in order to manage and operate its large and complex public infrastructure systems which our society relies on. Much of the information that was traditionally exchanged through human-communications can now be exchanged electronically through computer-to-computer data exchange. This allows for more extensive, rapid, and error-free exchange of information, but it requires more formal specifications and agreements to govern these data exchanges.

As a result, Maruleng Local Municipality has decided to develop a strategy that will lead to planning, executing, and implementing IT projects and policies that will see IT being leveraged in delivery of services to communities that it serves.

This document was developed to set out guidelines, standards, policies and procedures to give effect to the IT Governance Framework and provide guidance, roles, responsibilities, and rules on the use of information technology.

2. IT EQUIPMENT MANAGEMENT POLICY

2.1 Overview

The purpose of this policy is to provide the Maruleng Local Municipality with an IT Equipment Usage Policy in order to apply an effective and consistent standard for the IT equipment and software in use by the Department.

2.2 Purpose

The objectives of this policy are to:

2. 2.1 Clearly state rules governing usage of Maruleng Local Municipality computers and networks

2. 2.2 Encourage responsible and proper use of Maruleng Local Municipality information systems

2. 2. 2 Help ensure a Maruleng Local Municipality computer and network infrastructure that Supports Maruleng Local Municipality objectives and operational requirements

2.3 Scope

This policy applies to all Maruleng Local Municipality employees, contractors, service providers and others who are granted access to Maruleng Local Municipality information systems. This includes but not limited to computers, associated peripherals and software.

2.4 Policy Statement

2.5 Software

2.5.1 Software Installation

2.5.1.1 For purposes of complying with copyright laws and minimizing computer threats, only Maruleng Local Municipality authorised software must be installed on computers and this must be done by authorised IT Official only.

2.5.1.2 Computer users must not intentionally develop, use or distribute computer programs or software to disrupt other computer systems, information systems or damage software and hardware or bypass system security mechanisms and controls. More precisely, users must not use any software that may threaten the Confidentiality, Integrity and Availability of information and information systems. The use of any unauthorised or destructive program may result in legal civil action for damages or other punitive action by third parties, including Maruleng Local Municipality, as well as criminal action.

2.5.1.3 All divisions shall purchase computer hardware and software through IT Section. These divisions should clearly motivate the need for a particular software or hardware.

2.5.1.4 Software under testing or evaluation must under no circumstances be installed on production computers including computers, laptops and servers. Evaluation software must be installed on IT equipment designated as test equipment and whenever possible separated from the production network. IT Section has the sole authority to allocate IT equipment for testing purposes.

2.5.2 Software Change Control

2.5.2.1 All software shall be held in a lockable cabinet held at IT Section.
2.5.2.2 Software taken from the cabinet by authorised staff shall be recorded in a software register and upon return be signed back into the register.
2.5.2.3 IT Section shall license all appropriate software.
2.5.2.5 Should an official require specialized software than currently available; the official shall motivate this in writing coupled with authorisation from the official's supervisor. IT Section will at its discretion evaluate the merits of each software request.

2.5.3 Reporting of Incidents

Business Software Alliance randomly carries out audits to prevent illegal use of software and as a result hefty fines may be imposed for use of unlicensed software. Illegal use of any software must be reported to IT Section immediately.

2.6 Computer Equipment

2.6.1 Protection of IT Equipment Off-Premises

2.6.1.1 Users shall ensure that Maruleng Local Municipality IT equipment is protected while in use away from municipal premises regardless of ownership. The security of the equipment should wherever possible be equivalent to on-site use of the equipment.

The following applies to IT equipment away from the office:

2.6.1.1.1 Users shall not leave IT equipment unattended in public places;
2.6.1.1.2 By removing IT equipment from Maruleng Local Municipality premises, users acknowledge the increased risk of theft and/or loss, thus users must take all necessary precautions to protect and disguise this equipment. This can include using non-conventional laptop bags such as back packs and keeping equipment away from public eyes;
2.6.1.1.3 Only users who have been authorised to remove specific IT equipment from the premises, shall be allowed to use the equipment off-site;

2.6.2 Equipment Change Control

2.6.2.1 All problems and changes to the computer equipment must be registered with the IT Helpdesk.
2.6.2.2 No unauthorised staff may alter any software and hardware configuration.

2.6.3 Transfer of Equipment between Users

2.6.3.1 The transfer of IT equipment shall be managed by IT Section and all requests for transfers have to be submitted to IT Section and be recorded by asset management.

2.7 Standardisation of Hardware and Software

2.7.1 IT Section personnel shall from time to time, ensure that IT equipment in Maruleng Local Municipality is standardised as much as possible to minimise resources needed for

maintenance, therefore users shall be required to comply with any recommendations as prescribed by IT Section. Simply, this means that users will not bypass or attempt to bypass or disregard controls implemented by IT Section.

2.7.2 Additionally IT Section shall standardise computer software and hardware for users based on, but not limited to job function, division and the least privilege principle. This will help avoid unnecessary software license costs.

2.7.3 Should a user require specialised hardware than the current standard, the user shall motivate this in writing and authorised by the user's superior. IT Section shall at its discretion evaluate the merits of each hardware request.

2.7.4 Computer hardware shall only be modified by authorised IT Section staff.

2.7.5 All computers shall come standardised with Antivirus software to protect against viruses and malicious computer programs.

2.8 Stolen IT Equipment

Stolen IT equipment shall be reported to the Asset Management Section who will start with the process of recovering the stolen equipment.

2.9 Unattended User Equipment

2.9.1 It is the sole responsibility of users to ensure the protection of IT equipment which have been assigned to them by Maruleng Local Municipality. All laptop users shall be assigned with a laptop lock to prevent theft. Users shall ensure that they know how to physically secure their laptops. Offices, computer rooms and storage facilities shall also be locked when unattended. Failure to apply necessary protection for equipment shall constitute negligence and the user may be held liable for the loss.

2.9.2 Users shall terminate active sessions or log out of their computers whenever they are moving away from the workstation unless they lock the computer screen, in which case, they would be required to re-enter the password. No computer may be left unlocked.

2.10 Disposal and Reuse of Equipment

2.10.1 IT Computers and Laptops older than 5 years shall be disposed because they shall have exceeded their warranty cover. In this case IT Section shall take the sole responsibility of ensuring that all licensed software is removed and all stored information is securely overwritten. Any individual who disposes any IT equipment without the secure removal of data will be exposing Maruleng Local Municipality to compromised and unauthorised disclosure of information, thus will be in direct breach of this policy.

2.10.2 In cases where previously used IT equipment including laptops, personal computers or memory sticks are reassigned to another Maruleng Local Municipality employee, IT Section shall ensure that all information is securely deleted to protect the confidentiality of information.

2.11 IT Equipment by Category

2.11.1 Critical IT Equipment

To ensure that critical business activities take place and prevent loss, damage or compromise of critical assets, critical IT equipment shall be protected from various security threats and Environmental hazards. The following special controls shall govern the security of this critical equipment:

a. All critical system such as servers, switches, routers, printers used to print pay slips shall be stored in a physically secured environment protected by access control.
b. Owners of critical IT equipment shall implement the highest possible protection of these assets against failure, disaster, unauthorised access, tampering and periodically review security breaches and misuse.
c. Owners of critical IT equipment shall keep updated copies of configurations, operational procedures and usage guidelines to ensure continuity of operations after failures and prevent a single point of failure wherever possible.

2.11.2 Laptops/Notebooks

a. Officials that have been allocated or provided with laptops shall be responsible for the safety and custodianship of the laptop in the office and outside the office.
b. On connection to a local area network (LAN), a notebook that has been out of office shall be automatically updated with the latest antivirus signature file by a server. This is done in the background, and a user may not observe or be aware of this action.
c. All laptops allocated to users shall always be carried in a padded carry bag which is provided with the laptop.
d. Only licensed software shall be loaded on the laptops
e. Laptops shall be checked in and checked out by the security personnel at the entrance gates. They shall record the make, model and departmental inventory numbers in their register.
f. If a laptop or any of its accessories is lost due to outright negligence, the user will be required to pay a depreciated value of the notebook.
g. Standard configurations shall be maintained in all MLM laptops by IT Section and no user will be allowed to install their own software nor change configuration settings.
h. The following users shall be provided with laptops by default:

- Members of the Executive Council
- Heads of Departments
- Members of the Senior Management Service
- Heads of strategic business units
- Information Technology Officials
- Project Managers
- Process engineers
- And Researchers

2.11.3 Removable Media

Removable media such as memory sticks, DVDs and data compact discs are often the primary entry point of unauthorised software and viruses and a means of unauthorised information leakages. As a result, the following guidelines shall be followed when using removable media:

a. Users shall always scan removable media for viruses prior to use. This can be done simply by right clicking the removable media or CD icon in My Computer and selecting “scan for viruses”. Data on the media must only be accessed upon successful scanning or deletion of any viruses;
b. Users shall take the principles of least privilege into consideration when copying official information and data to removable media. This means that users are not allowed to copy information which they are not authorised to access. Additionally, users must take all necessary precautions to safeguard all classified or unclassified official data residing on removable media from unauthorised access;

c. Copyright laws also apply to copying of data to and from removable media. A user may be held liable for any copyright violations.

2.11.4 Printers

a. Users shall be required to share printers on the network based on physical proximity and division in order to avoid unnecessary costs.
b. Users of printers shall take into account that printer resources such as cartridges and papers are not infinite and refrain from misuse of printers and printing of personal documents.
c. IT Section shall ensure that all management interfaces of printers are protected by a password to prevent unauthorised use or configuration.
d. Recognising that documents can be processed and stored on computers, users shall take care to optimize printing resources by only printing when a paper copy is necessary.
e. Sensitive or classified printed documents shall immediately be removed from the printer after printing to prevent unwanted information disclosures.
f. Printers that are dedicated to printing confidential information such as pay slips, invoices and cheques shall be stored in areas where physical access is strictly controlled. These areas should be clearly marked to deter unauthorised access. It is the responsibility of each division to protect such sensitive printers.
g. Only authorised maintenance personnel shall carry out printer repairs.

2.12 Personal Use

While IT equipment is allocated to ensure that users have the necessary tools to carry out their official duties, it is inevitable that equipment will be used for personal use. While this is not prohibited, the use of IT equipment for personal use should be in a responsible manner that does not incur unnecessary costs to Maruleng Local Municipality. The following guidelines govern personal use of IT equipment:

2.12.1 Equipment should not be used to process, distribute or store any data or information protected by copyright laws/or intellectual property rights as this can lead to legal action;
2.12.2 Computers must not be used to play games or perform any activities that may contribute to decreased employee productivity.

2.13 House Keeping

Users shall use Maruleng Local Municipality IT equipment responsibly in line with the following housekeeping rules:

2.13.1 Offices with IT equipment shall be locked when leaving the office to prevent theft amongst other things;
2.13.2 IT Equipment shall not be placed next to heaters or air conditioners as humidity and heat can shorten the life of internal computer components;
2.13.3 Users shall not eat, drink or smoke next to IT equipment as this cause damage to the equipment and could be a health and safety risk;
2.13.4 Only damp cloths with suitable cleaning fluids shall be used when cleaning computer keyboards, screens, printers and other IT equipment;
2.13.5 Whenever possible, IT equipment shall not be connected to the same electric power as other power consuming devices. Red plugs should only be used for IT equipment;
2.13.6 For purposes of information backups, IT Section has put in place mechanisms to

synchronize information on the user's computer to a central file server. As a result, all files in the "My Documents" folder shall be backed up daily. Users shall not store any multimedia files like videos and music in this folder. These files shall be moved from this folder to the "C drive". It is the joint responsibility of the user and IT Section to ensure that these files are relocated.

2.14 Movement of IT Equipment to And from Municipality Premises

2.14.1 IT equipment shall not be moved from Maruleng Local Municipality premises without authorisation from Asset Management Section. This authorisation shall be in the form of a laptop card or an "Authority to remove IT equipment from Premises Form" obtainable from Asset Management Section.

2.14.2 All other IT equipment taken into Maruleng Local Municipality premises shall be signed in at security services at reception areas.

2.15 Computer User's Responsibilities

2.15.1 Users shall ensure proper use of IT equipment in accordance with all provisions of this policy.

2.15.2 Users are required to report any misuse of IT equipment or alert IT Section of potential threats to IT equipment.

2.15.3 It is the user's responsibility to seek guidance from IT Section or any related division in the department when in doubt of what constitute acceptable or prohibited use of IT equipment.

2.15.4 While security of IT equipment is the primary responsibility of Security Services, users must take note that they share this responsibility.

2.16 IT Section Responsibilities

2.16.1 IT Section shall implement mechanisms and technological controls to ensure, monitor and enforce compliance to this policy.

2.16.2 IT Section shall review this policy annually or when necessary to address new issues arising from the use of IT equipment.

2.16.3 IT Section shall investigate and follow-up on reported and suspected non-compliance and take necessary corrective actions.

3. USER ACCOUNT AND PASSWORD MANAGEMENT POLICY

3.1 Overview

Passwords are one of the primary mechanisms that protect potentially sensitive official information systems and other resources from unauthorized use. While passwords are not the most secured way of protecting information and information systems, constructing secure passwords and ensuring proper password management is essential. Poor password management and protection can allow both the dissemination of information to undesirable parties and unauthorized access to MLM resources. Poorly chosen passwords can be easily compromised. Password compromise can lead to inappropriate disclosure and use of MLM resources or sensitive information and also disclosure of personal information. Training users in the proper password creation and management greatly reduces these risks.

3.2 Purpose

The purpose of this policy is to establish minimum rules, guidelines and standards for passwords creation and management used to logon to MLM information systems.

3.3 Scope

This policy applies to all user accounts provided by MLM and all MLM employees, contractors and service providers that logon to MLM information computers and network.

3.4 Policy Statement

All user accounts used to logon to MLM information systems shall be protected with passwords. Furthermore, passwords must be changed regularly to avoid unauthorized access to information and information systems. Passwords that are not managed properly are at risk of accidental disclosure overtime.

3.5 Requirements

- Every user must have a unique username. For MLM employees, this shall be the user's surname and initials.
- Initial passwords must be uniquely created by a random password generator and must be communicated to the user in a secure manner.
- The user must automatically be forced by the computer system to change this initial Password. Upon initial user logon, Passwords may not be blank.
- To prevent accidental disclosures of passwords and unauthorized access to newly created user accounts, initial passwords can only be changed after a minimum of one day.
- No passwords will be stored in clear text or reversible encryption.
- The system administrator in charge of user management will only give initial passwords, unlock accounts or reset passwords once the password reset request form is completed and the identity of the user has been validated.
- If a user's password has expired, blocked and forgotten, then the user must complete a **password reset request form (ANNEXURE B)** and send it to IT Section for processing. This is to ensure that all requests to reset passwords are recorded for auditing purposes and to prevent unauthorized resetting of other individual's passwords. IT Official may at its discretion require the user requesting the request to physically present him/her self.
- Passwords used within MLM should not be used for external internet accounts and service providers.
- Passwords must not be included in any automatic login process.

3.6 Password Protection Guidelines

- Never write usernames and passwords on keyboards, walls, monitors, post-it notes, tables or any material. A memorized password is not prone to accidental disclosure.
- Your password is secure and must not be shared with anyone including but not limited to colleagues, managers and IT Official. This exempts generic departmental passwords i.e., passwords used and managed by a group in a specific department.
- Any file that stores passwords must be encrypted or password protected.
- Passwords or pass phrases must not be sent via email or communicated verbally except in cases of password resets and initial user creation between IT Section and the user involved.
- Passwords must be changed immediately upon disclosure or suspected disclosure.
- Passwords may not be written or saved in electronic documents unless these documents are encrypted and the user ensures that the encryption keys cannot be accessed by unauthorized individuals.
- Computers must be locked when the user moves away from the computer to prevent unauthorized access.

3.7 Password Guidelines

- Passwords must contain a mixture of special characters, alphanumeric characters in lower and upper cases e.g., P@s$w0Rd can be used instead of password.
- Pass phrases can be used instead of highly complex passwords to prevent the need to write the password where it can be accessed by unauthorized individuals, e.g. Take Cover can be converted to T@k3_Cov3r.
- Passwords from dictionaries in any language are easily guessable and should be avoided.
- Passwords should not be identical to the user ID, names, surname, computer name, job title or anything that a would-be password attacker can guess.

3.8 Password Construction Standards

- Passwords must consist of a mix of special and alpha-numeric characters.
- Passwords must not be the same as the username, first name, surname, street address or any words contained in a dictionary of any language.

3.9 Account and Password Protection

- A user account will be locked out indefinitely after three failed attempts in order to protect accounts and passwords from brute force attacks or password guessing. Upon account lockout, only the system administrator can unlock the account at the request of the user involved.

3.10 System-Based Password Requirements

- Privileged and administrative passwords must be subject to stringent composition and frequency of change. Privilege passwords include passwords for routers, switches, firewalls, network operating systems and any other IT resource.

3.11 Best Practices for System-Based and Server Passwords

- Privileged passwords should not be communicated via telephone, fax, email or any printed form.
- Administrator/privilege passwords must not be disclosed to external contractors.

- A number of shared local administrative passwords may be used on machines for specific divisions and computer networks.
- Service accounts must not rely on admin accounts/passwords.
- Passwords must be unique from all previous passwords.

3.12 System Administrators

- System administrators and those that have system administrator roles shall configure MLM information systems to comply with this Password Policy.
- System administrators and information security personnel should work with users in an effort to ensure that they are able to comply with this policy.

3.13 Application/Web Developers

- Application and Web developers developing applications that require password authentication shall create code that complies with this Password Policy.

4. IT SECURITY POLICY

4.1 Overview

Increasingly, departments and their information and communication systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, viruses, computer hacking and denial of service attacks. Dependence on information and communication systems and services means departments are more vulnerable to security threats. Management shall set a clear policy direction and demonstrate support for, and commitment to, information and communication system security through the issue and maintenance of this information and communication system security policy and standards across all Maruleng Local Municipality offices. This document shall be read in concurrence with the Minimum Information Security Standards (MISS).

4.2 Purpose

The purpose of this policy is to provide the Maruleng Local Municipality with an information and communication system security policy in order to apply an effective and consistent level of security to all information and communication systems that process Maruleng Local Municipality information.

4.3 Scope

This policy is applicable to all employees of the Maruleng Local Municipality, including learners and interns as well all other stakeholders who make use of the Maruleng Local Municipality IT network.

4.4 Policy Statement

This policy shall develop an information and communication system security culture that reflects a consistent approach, based on an understanding of the security issues and a cost-effective way of managing them. This will include reasonable level of protection to unclassified information so that Maruleng Local Municipality offices can exercise control over that information, particularly in relation to public release and be able to demonstrate accountability by a structured method of information and communication system security implementation and verification across Maruleng Local Municipality offices.

4.5 Information System Security

4.5.1 User Accountability

a. All users who access Municipal IT systems must be uniquely identified in order to detect and identify unauthorised access to the system.
b. It is the responsibility of Municipal IT systems users to safeguard the information handled in those IT systems
c. Users of the municipal IT systems shall report to IT Section any suspected breach or weaknesses to the systems security

4.5.2 Controlled access

a. Each user of MLM IT systems shall be granted access only pertaining to the scope of their jobs or tasks assigned to them at that particular moment.
b. IT Section shall ensure that access granted to the user cannot by any chance lead to information security violation.

c. User's specific duties and responsibilities shall be documented and signed and filled.

4.5.3 Levels of Protection

a. The sensitivity of the IT systems shall determine the level of protection required while taking into consideration the identified threats and potential vulnerabilities.

4.5.4 Disaster Recovery Plan

a. An approved Disaster Recovery Plan and procedures should be determined by the IT Section to specify the appropriate security measures to ensure the degree of confidentiality and integrity required for the recovery system.
b. The plan should also specify a regular procedure for making copies of data from which to recreate originals in case of disaster.
c. The MLM Disaster Recovery Plan must be tested regularly

4.5.5 Security Awareness

IT Officials should initiate security awareness programmes in order to foster the security awareness to the MLM users.

4.5.6 System Access Control and Password Security

a. Access to MLM IT systems shall be provided on a least privilege.
b. All MLM computers and laptops must be protected by approved password-based access control system.
c. Multi-factor authentication for remote access to MLM networks shall be implemented where applicable.
d. Each MLM IT system must have clear procedures for approval and method of granting access to the users.

4.5.7 Desktop and Laptop Security

a. Users must ensure reasonable physical security for Desktops or Laptops issued to them. The desktops and laptops should be in locked rooms with secured access control when not in regular use or at the end of working shift.
b. Laptops should be secured through the use of locking cables or in a locked drawer such that they cannot be removed.
c. All desktops and laptops must have a password access-controlled screensaver that automatically locks itself after a period of inactivity.
d. Users may not disable, uninstall, or interfere with software and systems that update, backup, encryption, or anti-malware services.
e. No users shall fix or fiddle with their broken or malfunctioning IT equipment. All broken or malfunctioning desktops and laptops shall be reported to IT Section to have them fixed or replaced.

4.5.8 Physical Security

a. Access to computer and server rooms and other areas containing sensitive IT information or computer-related equipment shall be physically restricted and they shall be controlled with electronic access control mechanism.
b. No MLM user shall leave IT equipment on desks unattended, especially during non-working hours.

c. Visitor access should be controlled

4.5.9 . Utilization of Private Computers

When private computers are used, written approval shall be obtained from Municipal Manager to use a private computer for official purpose. A computer register shall be established containing full personal particulars of the person, as well as details of the computer. Classified information bearing a sensitivity of Confidential or higher shall not be stored on a private computer.

4.6. IT Communication Security

Users must use communication channels authorised by MLM IT Section only. Those communication channels shall be set out depending on the type data or information to be communicated.

4.6.1 Security of Data Transmissions

a. Non-public data and information must be encrypted in order to protect it from being disclosed to unauthorised parties.
b. All MLM users are responsible for assessing confidentiality level of data being sent or residing on the IT equipment they use.

4.6.2 Modems/Dial-Up Communications

No modems shall be connected to communication networks without the authorization from IT Section. Authorisation shall only be given on receipt of a detailed motivation approved by the particular user's Senior Manager, requesting such facilities and a security plan detailing the manner in which the use of the modem and classified information transmitted through this modem will be regulated and controlled.

4.6.3 Electronic Mail

a. Electronic mail must be used solely for business communication purposes, and the information sent via electronic mail shall be treated with discretion and shall remail the property of the municipality.
b. No MLM user shall use the MLM electronic mail for personal communication.

4.7 IT Security System Controls

4.7.1 Security and Computer Viruses

In order to secure the network, it is necessary that:

a. If any desktop or laptop or server poses a risk to the network, other hosts or service delivery, the host shall be disconnected from the network until the risk has been resolved.
b. All desktops, laptops and servers shall use the latest security patch levels, as approved by IT Section.
c. The computer name of all desktops, laptops and servers shall contain the exact username of the owner, unless authorised by IT Section.
d. IT Section shall maintain virus-scanning software to protect the MLM network against any virus attacks.

4.7.2 Firewall and Perimeter Security

a. MLM IT Section must deny all internet traffic initiated from outside the MLM network unless explicitly permitted. Access may be permitted by IP Address, Port Number or other mechanism and access may be temporarily removed if a threat is detected.
b. Wireless devices and VPN access are not allowed on the MLM network, unless provided and authorised by IT Section.
c. VPN network extensions are only permitted making use of secure tokens, managed and supplied by IT Section.
d. Proxies allow the Municipality to account for bandwidth usage, so Firewall rules must be used to enforce the use of proxies.

5. INTERNET ACCEPTABLE USE POLICY

5.1 Overview

The World Wide Web is a worldwide network of computers that contains millions of pages of information. The internet is a necessary job-enhancing tool because it allows internet users access to information required to carry out and enhance their jobs when required. Recognising the importance of the internet, many organisations and government departments have implemented information systems to provide staff members with access to the internet.

However, an organisation which connects its networks to the internet exposes its information systems to all kinds of internet-borne security risks due to the open nature of the internet.

Furthermore, current-day applications like e-mail, www, etc. require relatively large amounts of bandwidth, of which the demand and cost is very high. As a result, organisations connected to the internet need to implement technical and procedural measures to mitigate risks from untrusted networks and to ensure that internet resources are utilized in a manner which does not adversely impact normal business operations.

5.2 Purpose

The objectives of this policy are:

a. To define security “laws and governance” that shall be enforced departmental wide to ensure that MLM internet information systems are adequately protected from misuse or direct/indirect exposure to security risks.
b. To ensure the highest possible level of Confidentiality, Availability, Reliability and Integrity for the MLM network, Information and information systems.
c. To encourage cost-effective and productive use of MLM internet systems.
d. To clearly define user responsibilities and liability when using departmental internet facilities in day-to-day activities.
e. To ensure compliance with regulations of RSA and other relevant international laws, regulations, standards and best practices.

5.3 Scope

MLM provides internet and World Wide Web access to all its employees and employees are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the internet. Even harmless search requests may lead to web sites with highly offensive and/or malicious content. Additionally, having a web-based email account on the internet may lead to receipt of unsolicited e-mail containing offensive and malicious content.

While MLM implements adequate measures to govern internet usage, employees are ultimately responsible for any internet-related activities and any material viewed or downloaded by users from the Internet. To minimize these risks, the use of the Internet facilities at Maruleng Local Municipality is governed by this Internet Acceptable Use policy

5.4 Policy Statement

Internet users are expected to use MLM’s internet facilities in a responsible manner which complies to the laws and regulations of RSA, other international laws as well as policies, standards and guidelines as set by MLM. Access to MLM’s internet facilities is a privilege that may be wholly or partially

restricted by the department without prior notice and without the consent of the internet user when required by and consistent with the law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to MLM procedures or, in the absence of such procedures, to the approval of the IT Section.

5.5 Methods of Connecting to the Internet

To ensure security and avoid the spread of viruses and other security threats, Users accessing the Internet through a computer attached to MLM's network must do so through the departmental Internet proxy server or other information security systems like firewalls, Intrusion Prevention Systems, etc. Every employee will use his or her network username and password to access the internet for accountability and reporting purposes.

Bypassing MLM's computer network security by accessing the Internet directly by modem, 3G cards, mobile phones connected to computers, non-departmental wireless networks or other means is strictly prohibited unless the computer you are using is not connected to MLM's network. Disabling of or subverting any security software installed on departmental computers shall also constitute breach of this policy.

5.6 Detection of Viruses

Files obtained from sources outside MLM, including fixed and/or removable disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by vendors, may contain security risks that may damage MLM's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-MLM sources, without first scanning the material with MLM approved virus checking software. If you suspect that a virus has been introduced into MLM's network, notify MLM IT Section immediately. If you are uncertain how to scan for viruses immediately contact IT Section for assistance.

5.7 External Email Accounts and Instant Messaging

While external web mail accounts are not disallowed, users must ensure that these email accounts are not used to distribute and/or store official information as this might lead to intentional/unintentional disclose of sensitive official information. Only departmental email systems must be used when distributing official information.

Due to high number of security risks associated with Instant Messaging applications line msn messenger, yahoo messenger, etc. users are not allowed to use and install any instant messaging application on departmental computers or networks.

5.8 Distribution of information and data

Without prior written permission from MLM, the MLM's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, trojan horse programs, etc.) or any other unauthorized materials.

Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the users or any other employee's job performance; b) have an undue effect on the computer or MLM network's performance; c) or violate any other policies, provisions, guidelines or standards of this agreement or any other of MLM. Further, at all times users are responsible for the professional, ethical and lawful use of the departmental internet facilities.

5.9 Communication of Official Information

Unless expressly authorized to do so, users are prohibited from sending, transmitting, or otherwise distributing official information, data or other sensitive/confidential information belonging to MLM through the World Wide Web.

Unauthorized dissemination of such material may result in severe disciplinary action and other appropriate actions under the laws and regulations of RSA or any international laws.

5.10 Discussion Groups

No MLM employee may in his/her official capacity create, participate in discussion groups on the internet without authorization from his or her manager.

5.11 Copyright Restrictions

Users may not illegally copy material protected under national and international copyright laws or distribute that material to other people. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not under official duties agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the Department.

5.12 Frivolous Use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all internet users have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer/network resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing online games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, accessing P2P networks/applications or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

5.13 Limitation of Privacy

Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should acknowledge and understand the openness and privacy issues relating to the internet and as such have no expectation of privacy in anything they store or distribute using the MLM's internet facilities.

User consents to allow authorized I.T personnel to access to and review of all materials created, stored, sent or received by User through departmental Internet facilities for the purposes of accounting, monitoring of policy compliance and internet usage statistics.

5.14 Discriminatory, harassing and/or offensive language

Users are to refrain from using obscene, defamatory, derogatory, discriminatory or any offensive language while using MLM's internet facilities as such actions could have serious criminal, civil and moral consequences.

5.15 Installation and Downloading of Software

Recognizing the many security risks on the internet, users are cautioned not to install or download any software from the internet as this might result in copyright violations, virus infections, and installation of adware, spyware and malicious monitoring software. Opening malicious web sites can often lead to automatic installation of malicious software and users are also cautioned not to agree to any automatic installation presented by web sites. If a user is uncertain about how to proceed, it is his or her responsibility to get advice from IT Section. A user knowingly downloads and installs any software from the internet that can compromise the MLM network, information systems or other users will be in violation of this policy.

5.16 Additional Connections to the Internet

The department offers additional tools like 3G cards to selected employees to help enable remote internet connection and access to emails from remote locations. It must be understood that the usage of these 3G cards are governed by this Internet Acceptable Use Policy and as such 3G users must ensure that they utilize these 3G cards for official purposes. 3G users are more vulnerable to virus attacks and other security risks from the internet as they are not protected by departmental information security systems. This means that a 3G user visiting malicious sites could unknowingly distribute security risks to other computers while connected to the MLM network. No internet user is allowed to configure or enable other connections to the internet via modems, wireless networks and cell phones on departmental computers. Any additional internet connections should be reported to IT Section.

5.17 Monitoring and Reporting

MLM accepts that the use of the Internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the Department. In addition, all of the department's Internet facilities are provided for primarily official purposes. Therefore, the Department maintains the right to monitor and log the volume of Internet and network traffic, including but not limited to Internet sites visited, files downloaded by users, etc. The specific content of any transactions will not be monitored unless there is a suspicion of improper use or policy violation. It may also be necessary for authorized I.T personnel to view the contents of employees' electronic communications and internet activity history in the course of problem resolution. I.T support personnel may not view an employee's electronic communication out of curiosity or at the request of individuals who have not followed the correct authorization procedures. Furthermore, internet activities will be logged for reporting/statistics purposes and provided occasionally or on demand to I.T management to enable proper implementation of systems that will cater for the future growth demands and to ensure ongoing availability, scalability and reliability of these systems.

5.18 Prohibited Use

5.18.1 Accessing streaming audio or video, play online games
5.18.2 Accessing chat sites
5.18.3 Installing and using instant messaging applications
5.18.4 Download of copyrighted material including videos, music, software or any intellectual property
5.18.5 Accessing web sites and material that may be offensive to other employees. This includes but not limited to pornography, hate speech web sites, criminal/illegal activities, etc.
5.18.6 Using the internet to conduct criminal or fraudulent activities
5.18.7 Using the internet to illegally monitor, gather information about any individual, entity or organization.
5.18.8 Using the internet to intentionally subvert security systems or initiate a denial of

service against any information system or network

5.18.9 Using the internet to conduct any personal business operations at the expense of the department's bandwidth and resources

5.18.10 Connecting to the internet via 3G while the computer or laptop is connected to the Departmental network.

5.18.11 Using the internet such that it interferes with employee productivity

5.18.12 Sharing of usernames and passwords used to access the internet with other people including employees

5.18.13 Distributing of passwords or any sensitive user account information through the internet

5.18.14 Impersonating, misrepresenting or suppressing a user's identity when accessing the internet

5.18.15 Using 3G cards for making telephone calls

5.18.16 Using the departmental internet facilities to intercept or disclose, or assist in intercepting or disclosing electronic data or information.

5.18.17 Accessing P2P networks and web sites

5.18.18 Using profanity, obscenities or derogatory, sexist, racist, highly sensitive, offensive or defamatory remarks while using the internet.

5.18.19 Using the internet to access malicious sites and download illegal material

5.18.20 Use of VoIP applications not necessary for official duties e.g., skype

5.19 Conditions for internet Access

An employee must sign and accept the conditions and liabilities of this internet acceptable use policy before being granted access to the network. If the internet user then violates any part of this policy, remedial actions such as revoking the user's internet access and/or disciplinary may be taken.

Depending on the outcome of the investigations the user may be required to reapply for internet access by filling in the relevant forms.

5.20 Authorisation Procedures

For purposes of ensuring proper use accountability, control and proper use of the Internet, every employee utilizing a departmental notebook, computer, 3G card shall sign an undertaking in the format Annexure B, through which, he/she will abide by the policy stipulations contained in this policy. This undertaking will be presented by IT Section or the Personnel Office to the employee. The signed undertaking will be filled in the staff file of the employee. IT/Personnel Office will take all steps to ensure that all the employees are provided with these undertaking forms. Failure to sign shall lead to existing internet access for that employee revoked.

5.21 Internet User's Responsibilities

All internet users are responsible, accountable and liable for all their activities while browsing the internet. As such the internet user has the following responsibilities:

a. Ensure that their usernames and passwords are kept secure and not shared
b. Fully comply with all aspects of this policy
c. Immediately alert IT Office (Information Security/Incident Response) about any misuse and non-compliance.
d. Duty not to waste computer/network resources
e. Understand that the information or data sent via the internet may/can be intercepted by other
f. individuals and ensure that they fully acknowledge this privacy concern.

6. SOFTWARE INSTALLATION POLICY

6.1 Overview

Allowing users to install software or any computer program on Municipal computing equipment opens the MLM IT Systems up to unnecessary exposure. If that happens, the MLM IT Systems will be exposed to the following:

a. Conflicting file versions or DLLs which can prevent programs from running
b. The introduction of malware from infected installation software
c. Unlicensed software which could be discovered in an audit, and
d. Programs which can be used to hack MLM network

Maruleng Local Municipality will ensure that all Municipal computers, systems, data and communications are protected from unauthorized access in order to prevent data loss.

6.2 Purpose

The purpose of this policy is to ensure that all users of MLM IT systems by the procedures outlined in this policy in order to minimize the risk of loss of program functionality, the exposure of sensitive information and data contained within Maruleng Local Municipality network, the risk of introducing malware, and the legal exposure of running unlicensed software.

6.3 Scope

This policy covers all IT Systems and equipment of Maruleng Local Municipality. IT Systems and equipment referred in this policy include computers, servers, smartphones, and other computing devices operating within Maruleng Local Municipality.

6.4 Policy Statement

The purpose of this policy is to establish guidelines to govern the installation of software and any other computer program on computers provided to users by Maruleng Local Municipality. No users will install software or any computer grogram on Municipal computing equipment operated within the MLM network. Software requests must first be approved by the user's manager and then be made to the IT Section in writing or via email. Software must be selected from an approved software list, maintained by the IT Section, unless no selection on the list meets the requester's need. The MLM IT Section will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

6.5 Approved Software Applications

a. MLM IT Section will ensure that there are licenses on all approved software application.
b. With the exception of anti-virus (which should be set for automatic updates), all software updates should be performed or set by IT Section to ensure compatibility with IT systems.

6.6 Prohibited Software

a. MLM IT Section shall make it impossible for users to distribute or use computer software and programs for reasons such as scanning networks, intercepting information or password capture.

b. Users must comply with copyright laws and respect the intellectual property rights of others.
c. Users shall not be found in possession of unlicensed software on MLM premises. Therefore, users who will be found in position of unlicensed or unauthorized copies of software will be disciplined as appropriate under the circumstances.
d. No users shall use unlicensed software on MLM IT Systems and equipment during the course of carrying out their employment.

6.7 Installation of Software

a. Only licensed software shall be installed on MLM IT Systems and equipment.
b. All installed software must not introduce technical problems that interfere with the proper functioning of other programs or MLM IT Systems.
c. All users will be responsible for checking for software problems/issues once installed and immediately report problems/issues to IT Section.
d. Software shall not be used on any university-owned computers or computing equipment in such a way as to be deemed inconsistent with the applicable copyright laws or licensing agreements.
e. No MLM software and programs shall be installed on personal computers and laptops.
f. MLM retains the rights of ownership for any software application and media purchased by the Municipality.

6.8 Responsibilities of IT Section

a. IT Section will install all software purchased by the Maruleng Local Municipality only on Municipality owned computers.
b. IT Section will account for all software installation media and copies of software licenses and EULA agreements.
c. Only IT Section will perform migration of software/programs and data from one MLM owned computer to another, as long as they are not personal computers or for personal use.

7. DATA CENTRE ACCESS CONTROL AND ENVIRONMENTAL POLICY

7.1 Review

Data Centers provide stable environments, enhanced security, equipment and alarms, uninterrupted UPS, high-speed network connectivity, and other features required by the critical resources they contain. The policies and procedures described in this document have been developed to maintain a secure, safe environment and must be adhered to by all users of MLM Data Center. All users requesting access or maintaining servers in the MLM Data Center must understand and agree to these procedures.

7.2 Purpose

The purpose of this document is to ensure the security and reliability of MLM IT Systems residing in the Municipal Data Center.

7.3 Scope

The scope of the policy will cover, but is not limited to the following areas:

7.3.1 Security
7.3.2 Safety measures and procedures
7.3.3 Emergency measures and procedures
7.3.4 Access control procedures
7.3.5 Change and configuration management
7.3.6 Environmental control, reporting and maintenance
7.3.7 Monitoring facilities.

7.4 Policy Statement

Access to MLM Data Center shall be documented in this policy and procedures and managed. Authorisation to the Data Center areas shall be granted and controlled by the MLM IT Section and it shall be granted only users whose job responsibility require access. Electronic access control systems shall be used to manage access.

7.5 Security

7.5.1 Entry Systems and Access Control

7.5.1.1 Access shall be controlled via Biometrics fingerprint system and all doors shall be fitted with sensors to detect unauthorised or prolonged opening.
7.5.1.2 Staff and visitors shall not adjust or otherwise tamper with door fittings. Any suspected faults with doors, lights or any security equipment should be reported to Security Services and/or IT Manager immediately.
7.5.1.3 Any person requiring access to the Data Centre shall sign the log book upon arrival.
7.5.1.4 Only authorised IT and Security Services personnel shall have access to the Data Centre via the biometrics system. Any other personnel including full time employees, contractors and vendors will be escorted by authorised IT and/or Security personnel during office hours.

7.5.2 Contractor Access after hours

7.5.2.1 MLM Security Services Provider shall be responsible for access control and security of the Data Centre outside normal working hours.

7.5.2.3 All contractors required to carry out some work on the data center outside normal working hours shall obtain authorisation from IT Section prior to their arrival on the Municipality premises and a copy of that authorisation must be given to the MLM Security Services Provider.

7.5.3 Close circuit television

7.5.3.1 MLM Security Services Provider shall monitor all entries and exits of the Data Center Areas by a Closed-Circuit Television (CCTV) to capture all movements into and out of the Data Center Area.

7.6 Safety

7.6.1 Signs and information

7.6.1.1 MLM Data Center shall have all necessary signage posted at its access points.

7.6.1.2 Information posts and general notices relating to data – its criticality and security measures shall be posted around in the Data Centre. The information posted will also include important detailed information on first aid, emergency contacts and general Health and Safety.

7.6.2 Health and Safety Considerations

7.6.2.1 Maruleng Local Municipality has a policy on Health and Safety and it shall govern health and safety measures in the Data Municipal Center.

7.6.3 Emergency Exits and Fire Alarm Procedures

7.6.3.1 Maruleng Local Municipality has a policy on Emergency Evacuation Procedures and it shall govern the reaction of users when the fire alarm is triggered Data Center areas.

7.6.4 Fire Detection and Fire Extinguishers

7.6.4.1 Fire and Smoke Detection System and Fire Extinguishers shall be fitted and linked to audible and virtual alarms. MLM Health and Safety policy and procedures shall govern the system.

7.6.5 Electrical Safety

7.6.5.1 Maruleng Local Municipality shall deploy the services of qualified and registered Electrical technicians in all electrical problems/issues encountered in the Data Center Areas. No unqualified users shall have access to and attend to the electrical systems.

7.7 Data Centre Use

7.7.1 Hours of Operation

7.7.1.1 All normal operations and maintenance in the MLM Data Centre area shall be conducted during Municipal normal working.

7.7.1.2 All operations and maintenance required to be carried out after normal working hours shall be authorised by the IT Official and all MLM users shall be notified via email and/or via all other authorised communication channels about the maintenance which will take place. They must be notified about the date, starting and finishing time of the maintenance, and the communication must also be sent out to the users to notify them if the maintenance process is finished and that the Data System is back online or still offline if maintenance is not finished.

7.7.2 Equipment Delivery

7.7.2.1 IT Section must always have a list of dated expected deliveries of Data Center equipment and an IT Official shall supervise the delivery and sign all relevant documentation pertaining to the delivered equipment.

7.7.2.2 It shall be the responsibility of IT Section to authorise any user to supervise, sign and receive the delivery in the absence of IT Officials.

7.7.3 Control of Equipment and Spares

7.7.3.1 IT Section shall dedicate an electronic access-controlled storage room for the storing of broken and unused equipment, and spares. All broken and unused equipment and spares from Data Center areas shall be removed from the data center into the storage room.

7.7.4 Prohibited Items

The following items are prohibited from the Data Centre:

7.7.4.1 Combustible materials such as paper and cardboard (except reference manuals as needed);
7.7.4.2 Food and drink;
7.7.4.3 Tobacco products;
7.7.4.4 Explosives and weapons;
7.7.4.5 Hazardous materials;
7.7.4.6 Alcohol, illegal drugs and other intoxicants;
7.7.4.7 Electro-magnetic devices that could cause interference with computer and telecom equipment;
7.7.4.8 Radioactive materials; and
7.7.4.9 Photographic or recording equipment (other than backup media).

7.7.5 Cables and Wiring

7.7.5.1 Maruleng Local Municipality Health and Safety policy also governs the processes and procedures on cabling and wiring. All cables and wires shall be clearly structured and labelled when running under the raised floor, wall, and equipment racks.

7.8 Environment

7.8.1 Air Conditioning

7.8.1.1 All MLM Data Center rooms/areas shall be fitted with air conditioning system which will deliver enough cooling in accordance with design specification.

7.8.1.2 All fitted air conditioning system shall be serviced and maintained on regular basis and Certificate of service and maintenance carried out shall be issued and filed by the Health and Safety Section and IT Section shall keep copy thereof.

7.8.2 CO2 Fire Extinguisher

7.8.2.1 A relevant Class of Fire Extinguishers with the relevant prescribed gas shall be determined and procured by the Health and Safety Section and shall be installed in the Data Centre rooms/areas.

7.8.2.2 All installed Fire Extinguishers shall be serviced as per the Health and Safety guidelines and Certificate of Service and maintenance carried out shall be issued and filed by the Health and Safety Section and IT Section shall keep copy thereof.

7.8.3 Power and lighting Provisioning

7.8.3.1 Relevant power sockets shall be constructed according to the Electrical guidelines and IT Section recommendations.

7.8.3.2 MLM Data Center rooms/areas shall have adequate power light to ensure clear visibility of all equipment in the Data Centre, and lights shall be switched off when there no access to and/or movements in the Data Centre.

7.8.4 UPS Provisioning

7.8.4.1 Maruleng Local Municipality shall deploy UPS system as a power backup on all major IT System equipment in the Data Center in order to sustain power to those equipment for a specific period of time to allow safe shutdown.

7.8.4.2 The UPS System in Maruleng Local Municipality shall be serviced and maintained on regular basis and Certificate of Service and maintenance carried out shall be issued and filed by the Electrical Section, and copies thereof shall be kept by Health and Safety and IT Sections.

7.8.5 Temperature and Humidity

MLM IT Section together with Health and Safety Section and Electrical Section shall establish and implement recommended standard temperature and humidity required to protect and maintain the health and safety and life span of Data Center IT Systems equipment. Temperature and Humidity monitoring devices shall be deployed to monitor temperature and humidity deviations.

7.8.6 Environment Monitoring

7.8.6.1 MLM Data Center rooms/areas shall be monitored around the clock to ensure that the environment does not become detrimental to the IT Systems equipment in the Data Center.

7.8.6.2 Monitoring shall include:

7.8.6.2.1 Temperature and Humidity alarms;
7.8.6.2.2 Fire and Smoke Detectors;
7.8.6.2.3 UPS malfunctioning or discharge during normal AC power operation; and
7.8.6.2.4 Daily monitoring.

7.8.6.3 Service and Maintenance shall be carried out on regular basis and Certificate of Service and maintenance carried out shall be issued and filed by the IT Sections, and copies thereof shall be kept by Health and Safety and Electrical Section.

7.8.7 Dust Prevention

7.8.7.1 MLM Data Center shall be a dust free area and it shall well ventilated to prevent dust from affecting and damaging IT Systems equipment.

7.8.8 Waste Disposal and Cleaning

7.8.8.1 MLM Data Center rooms/areas shall not be a place for waste disposal. It must at all times to kept clean and free from waste in order to avoid unnecessary fatal incidents that could damage the IT Systems equipment in the Data Center areas. All items that can generate dust and that are easily combustible should remain outside the Data Centre rooms/areas.

7.8.8.2 Waste bins shall be available outside the Data Centre rooms/areas main entrance for easy disposal of other items of waste.

7.9 Change and Configuration Management

7.9.1 It shall be the responsibility of the MLM IT Official to identify and authorise necessary changes and configurations required on the Data Center IT Systems equipment and systems.

8. IT CHANGE MANAGEMENT POLICY

8.1 Overview

Uncontrolled changes to IT systems and applications could potentially result in significant system disruption, data corruption or loss. A formalised IT change management processes and procedures should be designed to ensure that changes are authorised and operate as intended.

8.2 Purpose

The purpose of this policy is to define formal requirements to manage changes to MLM IT Systems and applications, in order to prevent unscheduled disruption, data corruption or loss.

8.3 Scope

This policy applies to:

a. All IT systems or applications managed by Maruleng Local Municipality that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.
b. All change requests to IT systems and applications, including standard, minor, major and
c. emergency changes.

8.4 Policy Statement

Maruleng Local Municipality formally manages changes to its IT Systems, Infrastructure and Resources in order to prevent disruptions to the stability or integrity of Municipal IT systems, applications and data.

8.5 Change Process

The Change Management Policy seeks to protect the computing environment from uncontrolled changes; to restrict service disruptions caused by necessary changes to defined low-use hours and to minimize the occurrence of unintended affects during the implementation of necessary changes.

8.5.1 Change Initiation

A change is initiated when the requirements for a change has been identified. This request for change can be initiated for the following reasons:

a. Change to infrastructure components.
b. Resolving problems or Upgrading system.
c. Project related activities.
d. Ad-hoc activities that influence service delivery.

8.5.2 Change Planning, Testing and Implementation

8.5.2.1 Change Planning

All changes, except standard changes, should be planned and reflect as a minimum the following:

- What will be changed;
- Role-players and their responsibilities;
- When will the change take place;
- Implementation plan;
- Version control;
- Rollback plan; and
- Impact on the IT Continuity Plan.

8.5.2.2 Testing of Proposed Changes

Changes shall, where possible, be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation. This is done in order to minimise the impact on MLM information and data system security. Where requested changes cannot be tested, the MLM should be satisfied that the proposed changes do not pose an unnecessary risk to the Municipal functionality or IT Systems infrastructure and environment.

8.5.2.3 Change Implementation

All changes that were tested and passed the testing shall be documented maintained by the IT Official.

8.5.3 Change Logging and Filtering

8.5.3.1 All change requests shall be logged on to the IT Section remedy system and it shall be the responsibility of the MLM IT Section to assess and implement the requested changes.

8.5.3.3 All requests shall be logged on to the IT Section using a Request for Change Form which will be completed for the following changes:

CLASS	ITEM	DEFINITION
Significant	Install	New requirement introduced
Minor	Move	Move of any component within the Infrastructure environment
Significant	Addition	Additional requirements (including releases and or upgrades) within the Infrastructure environment
Minor	Configuration	A change to the function or the assembly to the Infrastructure environment
Significant	Decommission	Removal of any component from the Infrastructure environment
Minor	Operational state	Change from the current operation state of a component within the Infrastructure environment

8.5.3.4 There are two change types that needs to be adhered to, based on the above classes and items:

CHANGE TYPE	DEFINITION
CAB Changes	For changes that need to be channeled via the CAB after which approval or rejection will be provided
Pre-approved changes	For changes that can take place without being channeled via the CAB, e.g. password resets / creation of new user accounts

CAB CHANGES	PRE-APPROVED CHANGES
May cause down-time on production systems	May not cause down-time on any system
May affect one or more SLAs	May not affect any SLA
May affect configuration information	May not affect any processes
May affect processes for services	
Changed with high risk involved	

8.5.4 Emergency Changes

8.5.4.1 In circumstances whereby an emergency change arises, MLM IT shall provide a change control mechanism to manage an emergency.

8.5.4.2 The following criteria shall be accepted as Emergency Changes

a. Production loss
b. Financial loss
c. Prevention of death
d. Legislation changes

8.5.5 Change Approval

8.5.5.1 MLM IT Section shall have a system in place to manage change approval and the correct workflow associated with the required approval. The level of approval to the change request shall be determined by the risks of the change:

CATEGORY	VALUES		
	1	2	3
1. Change Classification	Major	Significant	Minor
2. Priority	High	Medium	Low
3. Impact	Multiple districts	Single district	No impact
4. Implementation	Exceed 4 hours	Complex	Simple
5. Black out	Exceed 4 hours	Complex	Simple

8.5.5.2 The sum of the value of the five risk categories may determine the approval process:

Low risk	Greater than 10 = Minor Approval required
Medium risk	From 6 to 10 = Significant Approval required
High risk	Less than 6 = Major Approval required

8.5.5.3 The risk factor indicates the nature of the approval:

Minor Approval	The Chairperson of the CAB has delegated authority to approve and schedule changes to the Senior Manager: Information Technology and shall report back to CAB
Significant Approval	The change submitted shall be discussed at the CAB and relevant documentation are sent to CAB members before the meeting for assessment
Major Approval	IT OFFICIAL shall raise the Request for Change with the CAB. Approved changed must be passed back to the CAB for scheduling and implementation
Emergency Approval	Request for Change forms and relevant documentation are sent to CAB members for approval. A minimum of two members need to approve the change

8.5.6 Change Implementation

8.5.6.1 Once change requests are tested and approved, it shall be the responsibility of the IT Official to deploy correct workflow to ensure successful implementation of all changes as scheduled.

8.5.6.2 A detailed report and feedback regarding the success or failure of the change implementation shall be documented and presented to the CAB within 5 days after the planned completion time.

8.5.7 Change Review and Reporting

After the changes have been implements, the IT Official shall conduct an evaluation of the changes implemented in order to:

8.5.7.1 Establish if the change implemented served the purpose and met the desired expectations

8.5.7.2 To ensure and assign follow-up tasks and actions to correct any problems or inefficiencies that may have arisen after the implementation of the changes in order to improve the future approach to change process.

8.5.8 Communication

Change process shall be managed and communicated from the early stage of request to the final state of implementation and review through all communication channels set out and approved by the Municipality. Communication shall include:

8.5.8.1 Change approvals
8.5.8.2 Change notifications
8.5.8.3 Change control escalations
8.5.8.4 Change management processes and procedure changes
8.5.8.5 Change management standard changes
8.5.8.6 Change management policy changes.

8.6 Roles and Responsibilities

Ownership of the change process and responsibilities of the parties to be involved in the process shall be identified and managed successfully.

8.6.1 Change Management

The manager for change management shall be responsible for:

8.6.1.1 Defining and establishing processes, procedures, division of work and the roles and responsibilities within the process workflow.
8.6.1.2 Ensuring conformance to documentation standards and agreed procedures.
8.6.1.5 Communicating all updates and/or changes of the Change Management Processes and Procedures.

8.6.2 Change Advisory Board

The MLM IT Section shall formulate a Change Advisory Board to function within the following mandate:

8.6.2.1 Review all high impact changes to be implemented
8.6.2.2 Review any change that was implemented unsuccessfully or had to be cancelled
8.6.2.3 Screen all the changes to ensure the correct category, type and item have been selected.
8.6.2.4 Monitor routine and low impact changes.

8.6.3 IT Official

8.6.3.1 Implement Change requests as per above mentioned Change Management Process
8.6.3.2 Provide regular feedback on progresses and procedures regarding the change request and schedule.

8.7 Change Lead Times

8.7.1 MLM IT Section shall set out change lead time and the lead time shall be monitored and strictly managed in order to ensure that the change process runs and stays within the constraints of the budget and time line.

8.7.2 All changes to be submitted shall be done within the following lead time matrix:

SERVICE	LEAD TIME
APPLICATION SYSTEMS	
New Application Releases	1 month
Incident Fixes	12 – 24 hours
Emergencies	12 hours
OPERATIONS	
Installation of hardware	1 – 2 months
Consumable – tapes / cartridges	2 weeks
Changes to Schedules	48 hours
Hardware maintenance	1 month
Changes to operation of servers	1 week
NETWORK	

Installation of new data lines	4 months
In- and outdoor transfer of data lines	1 month
Installation of new equipment on existing network	2 weeks
Incident fixes	3 weeks
TECHNICAL SUPPORT	
New application release	3 weeks
Environmental changes	2 months
Incident fixes	24 – 48 hours
Software evaluation	2 weeks
The lead time for non-standard changes that require research shall be negotiated with SBU's concerned, and will depend on the nature and complexity of the change or captured in Operational Service Level Agreements	

9. FIREWALL POLICY

9.1 Overview

Maruleng Local Municipality has an obligation to provide appropriate and adequate protection of its IT Systems and Infrastructure, including but not limited to Servers (Virtual and Physical), Network components, End User Computing Devices, Mobile Phones and Tablets. The Municipality has the responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems. Effective implementation of this policy shall reduce the likelihood of compromise which may come from a malicious threat source.

9.2 Purpose

Firewalls are an essential layer of Maruleng Local Municipality's IT Systems and Security infrastructure and the Municipality shall subscribe to a layered defense or defense-in-depth approach to network security. Therefore, the purpose of this Policy shall outline the requirements for deployment, management and operation of key firewalls in Maruleng Local Municipality.

9.3 Scope

This Policy applies to all firewalls and virtual firewall segments protecting the MLM IT Systems. If any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail, unless the Policy provision is required by law, in which case the Policy provision will prevail.

9.4 Policy statement

This Policy outlines key requirements for firewalls in scope as detailed in the Standards for Firewall Deployment and Management. These Standards must be adhered to at all times.

MLM servers must be protected with network perimeter and host-based firewalls. It shall be the responsibility of the MLM IT Section to deploy and administer network perimeter firewalls.

Web application firewalls must be deployed to protect the core applications as necessary.

Firewalls must be deployed to protect the MLM IT Systems from intrusion, suspicious irregularities, threats and block harmful traffic.

9.5 Requirements

9.5.1 The Firewall system shall control all traffic entering and leaving the Maruleng Local Municipality Internal network.

9.5.2 Maruleng Local Municipality Firewall shall block all incoming and outgoing traffic by default.

9.5.3 Only authorized incoming and outgoing traffic shall be allowed to pass through Maruleng Local Municipality Firewall.

9.5.4 Traffic with invalid source or destination addresses shall always be blocked.

9.5.5 Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid "external" address) shall be blocked at the network perimeter.

9.5.6 Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address) shall be blocked at the network perimeter.

9.5.7 Outbound traffic with invalid source addresses shall be blocked.

9.5.8 Incoming traffic with a destination address of the firewall itself shall be blocked unless the firewall is offering services for incoming traffic that require direct connections.

9.5.9 Traffic from outside the network containing broadcast addresses that are directed to inside the network shall be blocked.

9.6 Operations

9.6.1 Only Firewall system administrators shall be permitted to logon to Firewall hosts. Access to Firewall hosts shall be tightly controlled. Only Firewall system administrators are allowed to have user accounts on Firewall hosts. Firewall system administrators shall have personal accounts; i.e. no group logins are allowed.

9.6.2 All changes to Firewall access rules shall be made through a single approved interface. The Firewall shall have a trusted path for its management e.g. a physically secure dedicated management process with a password-based identification and authentication system.

9.6.3 Only Firewall system administrators with the appropriate authorisation shall make changes to the Firewall access rules, software, hardware or configuration. All changes shall be as a result of a request recorded in a Change Management System although emergency modifications can be requested by phone, with a follow up email and change request. Only authorised personnel must be able to implement the changes and an audit log must be retained as per the Departmental IT Change Management Policy.

9.6.4 Logging and audit facilities provided by the Firewall system shall be fully utilised. All significant traffic through the Firewall shall be logged. The Firewall shall provide sufficient audit capacity to detect breaches of the Firewall's security and attempted network intrusions. Firewall System Administrators shall examine logs on a regular basis and also set up mechanisms to respond to alarms.

9. 7 Configuration

9.7.1 The perimeter Firewall system shall be configured to deny any service unless it is expressly permitted. If there are no rules defined for the department network address, then traffic to or from that address shall be denied. Access to the department network shall be blocked during the start-up procedure of the Firewall.

9.7.2 The Firewall operating system shall be configured for maximum security. The underlying operating system of Firewall hosts shall be configured for maximum security, including the disabling of any unused services.

9.7.3 The Firewall product suite shall reside on dedicated hardware. Applications that could interfere with, and thus compromise, the security and effectiveness of the Firewall products, shall not be allowed to run on the host machine.

9.7.4 The initial build and configuration of the Firewall shall be fully documented. This provides a baseline description of the Firewall system to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state is maintained.

9.7.5 Security shall not be compromised by the failure of any Firewall component. If any component of the Firewall fails, the default response will be to immediately prevent any further access, both outbound as well as inbound. A Firewall component is any piece of hardware or software that is an integral part of the Firewall system. A hardware failure occurs when equipment malfunctions or is switched off. A software failure can occur for many reasons e.g., bad maintenance of the rules database on the Firewall or software which is incorrectly installed or upgraded.

9.7.6 There shall be regular reviews to validate the Firewall system meets the needs of the business regarding information security. The configuration of the Firewalls shall be regularly checked to ensure they still match the business requirements regarding the

security. It may be necessary to implement separate Firewall modules to protect against the vulnerabilities of certain services. An example would be a package to scan email for viruses or other malicious software. The Firewall must also be regularly tested for vulnerabilities. Applications on internal hosts that handle incoming services will need to be checked for known vulnerabilities.

9.8 Audit and compliance

9.8.1 Regular testing of the Firewall shall be carried out. The Firewall shall be regularly tested for;

- Configuration errors that may represent a weakness that can be exploited by those with hostile intent.
- Consistency of the Firewall rule set.
- Secure base system implementation

9.8.2 The Firewall system shall have an alarm capability and supporting procedures. When an agreed specified event occurs, an alarm shall be sent to the security team. Documented procedures shall exist to permit an efficient response to such Firewall security alarms and incidents. In the event that the Firewall itself is the subject of malicious attempts to penetrate it and the Firewall has the capability, delivery of services should be terminated rather than permit uncontrolled access to the department network.

9.8.3 There shall be an active auditing/logging regime to permit analysis of Firewall activity both during and after a security event. An audit trail is vital in determining if there are attempts to circumvent the Firewall security. Audit trails must be protected against loss or unauthorized modification. The Firewall system must be able to provide logging of specific (or all) traffic when suspicious activity is detected.

9.9 Responsibilities

IT OFFICIAL will be the sole responsible entity for putting in place firewalls and the management thereof. The monitoring will be done by IT OFFICIAL and reported to Risk and Security management if any breach attempts are detected.

9.10 Change control

With any Firewall it is very important to have change control. When rules are introduced there should be a well-defined method for documenting these and in the case of temporary rules, the removal date for the rule should be added in a comment field. The only way of checking if the Firewall is actually enforcing the agreed policy is to either verify it with an Intrusion Detection System, or to do a manual verification using a penetration test or a Firewall review by third party.

9.11 Monitor stability

A Firewall is like any other infrastructure component and should be managed as such. It should be monitored for availability to ensure maximum uptime. If a Firewall isn't stable, people will find ways of avoiding the Firewall that leads to a low level of security.

10. IT PATCH MANAGEMENT POLICY

10.1 Overview

Maruleng Local Municipality has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems onsite, offsite and inclusive of systems and services supplied by the third parties. Patch management is an area of systems management that involves acquiring, testing and installing multiple patches (software updates/code changes), to an administered computer system. MLM IT Section shall ensure that patches are installed properly, and all associated procedures are documented.

All system components and software shall be protected from known vulnerabilities by installing applicable security patches. IT Systems components and devices attached to the MLM network shall be regularly maintained by applying critical security patches within thirty (30). Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal IT Systems maintenance and support operating procedures.

Effective implementation of this policy reduces the likelihood of IT Systems compromise from a malicious threat actor or threat source.

10.2 Purpose

The purpose of this patch management policy is to enable Maruleng Local Municipality to ensure that IT Section is fully aware of the requisite security needed to patch a digital asset and describe the patching controls and constraints to minimize information security risks that may affect MLM IT System equipment.

10.3 Scope

This policy applies to computers (desktops and laptops), servers, networks, hardware devices, software and applications owned and managed by Maruleng Local Municipality, and all IT Systems that contain MLM data owned and managed by the Municipal IT Section.

10.4 Policy Statement

Maruleng Local Municipality IT Systems equipment must be protected by all means and listed by a rigid and reasonable patching activities. Vulnerabilities should be patched adequately. Maruleng Local Municipality has the right to protect its IT System equipment and ensure its compliance.

10.5 General Principles

10.5.1 Vulnerability Scanning and Analytics

In the face of so many patches being issued on a daily basis, MLM IT Section has no choice but to prioritize where it's going to invest its patching resources. Thus, a key component of any integrated patch management system must be automated vulnerability scanning and targeted assessment of the importance of MLM vulnerability.

10.5.2 Patch Process Governance

When analyzing security breaches, the root cause is often that: somebody did not install a patch; somebody waited for permission to install a patch, and the permission did not

arrive; or somebody was not even aware that the vendor had issued a patch. In other words, the process was not properly defined, or the process was not followed. Thus, MLM IT Section shall manage the patch process in order to provide an effective patch management solution.

10.5.3 End-to-End Patch Workflow Automation

Automated patch management is not just about deploying patches. MLM IT Section shall have an entire patching workflow that includes steps to be taken prior to and after installing a patch, such as performing patch pre-checks, implementing a rollback plan if a patch causes problems, restarting the system, and so on.

10.6 Monitoring

Maruleng Local Municipality IT Section shall be responsible for the administration of all IT Systems and will be required to compile and maintain monthly 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.

10.7 Assessing and Classifying Risk

MLM IT Section will ensure that all new patches identified are assessed I order to establish their level of criticality and relevance to Municipal IT Systems. The following shall be taken into consideration when assessing the patches:

- Emergency - an imminent threat to MLM computer network
- Critical – targets a security vulnerability
- Not Critical – a standard patch release update
- Not Applicable

10.8 Testing

a. All newly identified patches shall be download and reviewed based on the MLM defined risk matrix in order to establish the effect the patch on Municipal IT Systems prior to deployment.
b. IT Solution shall create a testing environment on its IT Systems for testing patches before they can be deployed on the live/production systems environment.
c. It is the responsibility of application users to identify any problem(s) with a patch(es) deployed in their IT equipment and to notify MLM Section of the problem(s). Applications and their users need to be defined and listed in the Configuration Management database.
d. If patch(es) is/are tested and failed, such patch(es) shall not be deployed and IT Section shall seek alternate means to patch the system.

10.9 Authorisation and Notification

a. MLM IT Official must get approval and authorisation from his/her Director and Municipal Manager prior to implementation.
b. Any deployment of patch(es) shall be communicated to the users prior to deployment because security patch may cause a system to malfunction.
c. IT Section shall determine timeframe and the emergency level for installing Critical and Non-critical security patches.
d. All patches that cannot be deployed with automated patch management solutions will be deployed manually within the timeframes and requirements laid out in this policy.

10.10 Verification

a. Network-wide audit scans must be conducted on all IT Systems on regular basis, and audit reports are to be kept for a period determined by the Municipality.
b. It is the responsibility of IT Section and users to verify and confirm the successful installation of the patch and advice any adverse effects.

10.11 Contingency Planning

a. All IT Systems equipment that are sometimes carried out of the Municipality Computer network coverage area must have patch management solution configured in them I order to automatically download and install approved patches when they physically connect to the MLM computer network.
b. In the event that a critical patch cannot be centrally deployed, it must be installed manually or via a vendor-maintained update site.
c. MLM IT section must always have IT Officials on standby to assist with manual deployment of patch(es).

10.12 Responsibilities

10.12.1 Municipal Manager

a. It shall be the responsibility of the MM to support the establishment of this patch management policy and procedures within the MLM.
b. MM shall ensure that funding and IT Officials are provided to effectively maintain municipal-wide patch management solutions.

10.12.2 IT Section

a. MLM IT Section shall ensure that policy is adhered to when deploying patch(es).
b. Monitor and identify any potential threats and vulnerabilities by reviewing current threats and vulnerabilities.
c. Ensure compliance to this policy by deploying an approved automated patch management solution in order to promote efficiency for all MLM IT Systems and monitor status of those systems.
d. Any deployment of patch(es) must be developed in an electronic database to maintain and track status of all patch actions and vulnerability corrections and to provide rapid response to internal or external reporting requirements.
e. Run patch management status report on monthly basis to using the Patch Management Compliance Form.

10.12.3 All Users and Third Parties Contracted To MLM

a. Must abide by this Patch Management Policy and all other applicable IT policies.
b. Must report any suspected non-compliance of this policy to MLM IT Section.

10.12.4 Maruleng Local Municipality

a. Reserves the right to monitor for violations of this policy.

11. ANTI-VIRUS POLICY

11.1 Overview

A virus is a piece of self-replicating code, most often a malicious software programme designed to destroy or corrupt information, steal user data or adversely impact the usage of IT systems. Potential sources of viruses include shared media such as USB memory sticks, electronic mail (including, but not limited to, files attached to messages), malicious code embedded in websites and software or documents copied over networks such as the internal network or the internet.

In addition, viruses spread from Maruleng Local Municipality could potentially lead to serious issues of damage to reputation and possible litigation.

This policy defines anti-virus policy on every IT System equipment including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content.

11.2 Purpose

One of the goals of Maruleng Local Municipality IT Section is to provide a Municipal computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by MLM users to help achieve effective virus detection and prevention.

11.3 Scope

This policy describes the measures taken by Maruleng Local Municipality to counter malicious software and the responsibilities of users, departments and IT Services in protecting the Municipality against viruses.

This policy applies to all users using MLM computers connected to the Municipal computer network via a standard network connection, wireless connection, modem connection, or virtual private network connection.

11.4 Policy Statement

a. The most current available version of the anti-virus software package used at Maruleng Local Municipality will be taken as the default standard.
b. All computers attached to the MLM computing network must have standard, supported antivirus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.
c. Any activities with the intention to create and/or distribute malicious programs onto the Municipal network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.
d. If a user receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the IT Section immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
e. No user should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT Section.

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

11.5 Rules for Virus Prevention

a. Always run the standard anti-virus software provided by Maruleng Local Municipality.
b. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
c. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.
d. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
e. Files with the following filename extensions shall be blocked by the e-mail system: [.exe, .bat etc.]. Business files with banned extensions shall be sent/received by compressing the same in a folder by use of a file compression utility.
f. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
g. Avoid direct disk sharing with read/write access. Always scan any storage media for viruses before using it.
h. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
i. Back up critical data and systems configurations on a regular basis and store backups in a safe place.
j. Regularly update virus protection on all MLM users' computers. This includes installing recommended security patches for the operating system and other applications that are in use.

11.6 IT Section Responsibility

The following activities are the responsibility of the Maruleng Local Municipality IT Section:

a. The IT Section is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted at IT Section's Shared Folder and the Municipality's Intranet and Website. Check one of these locations regularly for updated information.
b. The IT Section will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use. This is to be accomplished through the appointed Anti-Virus Server, which grabs all updates whenever released by Anti-Virus vendor and distributes to clients and can also push the Anti-Virus protection client installations to workstations, laptops and servers.
c. The IT Section will apply any updates to the services it provides that are required to defend against threats from viruses.
d. The IT Section will install anti-virus software on all Maruleng Local Municipality owned and installed desktop workstations, laptops, and servers.
e. The IT Section will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT Section may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.
f. The IT Section will perform regular anti-virus sweeps of Windows desktop OS and user files.
g. The IT Section will attempt to notify users of Maruleng Local Municipality IT Systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

11.7 Department and Individual Responsibilities

The following activities are the responsibility of Maruleng Local Municipality departments and users:

a. Departments must ensure that all of their departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.
b. Departments shall all users to use their personal computers for business purpose.
c. All users are responsible for taking reasonable measures to protect their IT Systems equipment against virus infection.
d. Employees must not attempt to either alter or disable anti-virus software installed on any IT Systems equipment attached to the MLM computer network without the express consent of the IT Section.

12. DATA BACKUP POLICY

12.1 Overview

A backup policy provides the last line of defense against data loss and is sometimes the only way to recover from an IT Systems hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document. A company's backup policy is among its most important policies.

12.2 Purpose

The purpose of this policy is to outline the processes and procedures in place for the MLM IT Section to backup and restore electronic data lost in the event of system or user error.

12.3 Scope

The intended coverage of this policy is all critical electronic data stored on the MLM computer network or network enabled equipment. Any resources saved locally to equipment hard drives will not be part of the backup process.

12.4 Policy Statement

All Municipal data residing on IT Systems maintained in the MLM Data Center must be copied onto Storage media on a regular basis for the purpose of disaster recovery and business continuation. This policy outlines the minimumrequirements for the creation and retention of backups.

12.5 Identification of Critical Data

The MLM IT Section must identify what data is most critical to the Municipality. This can be done through a formal data classification process or through an informal review of information equipment. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

12.6 Backup Frequency

Backup frequency is critical to successful data recovery. The following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup official:

- Incremental: Every Day
- Full: Every Week
- 2 weeks of data will be kept on disk for instant restores.
- 1 year of data will be kept on tapes located off site.
- Daily incremental and weekly full backups will be replicated to the secondary data center for disaster recovery purposes.

12.7 Data to be Backed Up

This backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

- All data determined to be critical to MLM operation and/or MLM user job function.
- All information stored on the MLM file server(s) and email server(s) (It is the user's responsibility to ensure any data of importance is moved to the file server.)
- All information stored on MLM network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

12.8 Data not to be Backed Up

Data the IT Department will not be responsible for backing up is as follows:

a. Users' personal data
b. Data stored to local hard drives of desktops and laptops
c. Data on removable media (i.e. DVD's, CD's, and Thumb Drives)
d. Data stored on mobile devices

12.9 Excluded extensions

On home directories folders ("My Documents") not all files will be backed up; the following are extensions that will be omitted:

- Mpeg
- Mpa
- Mp2
- Mp3
- Mp4
- Exe
- Vob
- Wsf
- Wma
- Wav

12.10 Backup Storage

Storage of backups is a critical issue and one that requires careful consideration. Since backups contain critical, and often confidential data, precautions must be taken that are appropriate to the type of data being stored. The IT Section shall set the following guidelines for backup storage:

When Municipal data stored onsite, backups should be kept in an access-controlled area. When shipped off-site, a hardened facility (i.e., commercial backup service or safe deposit box) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media. Online backups are allowable if the service meets the criteria specified herein.

12.11 Off-Site Rotation

Geographic separation from the backups must be maintained, to some degree, in order to protect it from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the Municipality's uptime requirements. The Maruleng Local Municipality shall determine the frequency in which the backup media must be rotated off-site.

12.12 Restoration Procedures and Documentation

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is conducted, under what circumstances it is to be conducted, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not

a. Misinterpreted by readers other than the backup administrator, and
b. Confusing during a time of crisis.

12.13 Restoration Testing

Since a backup policy does no good if the restoration process fails, it is important to periodically test the restore procedures to eliminate potential problems. Backup restores must be tested when any change is made that may affect the backup system.

12.14 Expiration of Backup Media

Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

13. DISASTER RECOVERY POLICY

13.1 Overview

Since disasters happen so rarely, most businesses often ignore the disaster recovery planning process. It is important to realise that having a contingency plan in the event of a disaster will give Maruleng Local Municipality a competitive advantage. This policy requires the Municipality to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

13.2 Purpose

The purpose of this policy is to define the need for Municipal Management to support ongoing disaster planning for Maruleng Local Municipality.

13.3 Scope

Due to the uncertainty regarding the magnitude of any potential disaster in Maruleng Local Municipality, this policy will only address the recovery of IT Systems under the direct control of MLM IT Section and that are critical for Municipality business continuity. This includes the following major areas:

a. Authentication, single-sign-on, and network directory services
b. On-premises enterprise applications (e.g. EMS)
c. Datacenter (Computing Services)
d. On-premises website and services
e. IT Systems equipment
f. Data networks and telecommunications (wired and wireless networks, file services, telephony)

This policy covers all phases of any MLM IT related disaster occurring at Maruleng Local Municipality. These phases include:

a. Incident Response
b. Assessment and Disaster Declaration
c. Incident Planning and Recovery
d. Post incident Review

13.4 Policy Statement

Corporate management has approved the following policy statement:

a. The company shall develop a comprehensive IT disaster recovery plan.
b. A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
c. The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
d. The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
e. All staff must be made aware of the disaster recovery plan and their own respective roles.
f. The disaster recovery plan is to be kept up to date to take into account changing circumstances.

13.5 Principles

Disaster Recovery planning is a program that has a continuous lifecycle. Detailed requirements for each of these steps are below. The high-level process for DR Lifecycle is as follows:

13.5.1 Roles and Responsibilities

13.5.1.1 The IT Section is responsible for:

a. Ensuring the MLM IT disaster recovery planning program is established and implemented in compliance with MLM laws and regulations.
b. Enforcing MLM users' compliance to Municipal IT Disaster Recovery Guidelines.
c. Developing policy, guidelines, best practices, IT disaster recovery planning, and incident response capability.
d. Ensuring that MLM IT Disaster Recovery Plans are maintained and exercised at appropriate intervals.

13.5.1.2 Municipality Leadership is responsible for:

a. Completing or assisting in the completion of the Business Impact Analysis.
b. Defining the maximum amount of tolerable downtime for each of the identified functions. This becomes the recovery time objective for the recovery solutions developed.
c. Defining the point in time to which data must be restored in order to resume processing. This becomes the recovery point objective for the recovery solutions developed. (i.e. how recent must the data used in the recovery be?).
d. Using input from information gathered in the Business Impact Analysis, the Recovery Time Objective, and the Recovery Point Objective to define recovery priorities to be used in developing recovery procedures.
e. Wording contractual and service level agreements with external entities in a manner that ensures compliance with these guidelines.

13.5.1.3 Disaster Recovery Team

a. A Disaster Recovery Team (or teams) must be selected, trained, and ready to deploy in the event of a disruptive situation requiring plan activation. Team members must understand their role on the team and the procedures necessary to execute the DRP.
b. The team must have a team leader that directs overall activities and keep appropriate management briefed.
c. Planners should understand that some or even most of the Disaster Recovery team members could be unavailable in the event of an emergency. The line of succession to identify team members responsible to assume authority for executing the IT disaster recovery plan in the event key designated team members are unavailable or unable to do so should also be determined and included in the plan.

13.6 Development of Disaster Recovery Strategies

The purpose of this policy is to document the recovery strategies and create a road map of predetermined actions that will reduce required decision-making during a disaster and systematically provide a documented recovery path. Although the likelihood of a catastrophic disaster is remote, the devastation and potential loss of the ability to perform services requires that advance planning occur in order to respond in an effective and responsible manner.

The recovery strategies developed should provide a means to restore IT components quickly and effectively following a service disruption. The selected recovery strategies should align and address the Business Impact Analysis and Risk Assessment findings.

13.7 Backup Procedure

MLM IT Section shall specify backup frequency based on data criticality and the frequency that new data is introduced. Backups should occur daily (at a minimum). Backup processes and procedures should designate the location of stored data, retrieval procedures, backup test procedures, file naming conventions, media rotation frequency, method for transporting data off-site, and a description of off-site storage facility.

The following should be included in the backups located off-site:

a. Copy of IT Disaster Recovery Plan
b. Data files (e.g., daily, weekly, monthly, etc.)
c. Program files and source code
d. Procedures and Scheduling instructions
e. Software licenses

13.8 Testing Backup Procedure

Prior to implementation of this policy, MLM IT shall the backup procedure. The test should include the successful restoration of data. This includes retrieval procedures to obtain off site data. The testing will also identify missing files, missing applications, and faulty procedures. Testing backup procedure will also increase the likelihood of discovering procedural inconsistencies before an emergency, rather than during one.

13.9 Offsite Storage Considerations

The following should be considered when selecting an offsite storage facility:

Geographic area - distance from Maruleng Local Municipality and the probability of the storage site being affected by the same disaster.
Accessibility - length of time allowable to retrieve data from storage and storage locations hours of accessibility.
Security - security capabilities of the storage facility and MLM user confidentiality must meet the data's sensitivity and security requirements
Environment - structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention/suppression, and power management controls)
Cost - costs of shipping, operational fees, and disaster response/recovery services.

13.10 Emergency Management

a. The IT Disaster Recovery Team, along with the MLM IT Section shall be responsible for overseeing IT Disaster Recovery activities in the event of an emergency.
b. There must be processes and procedures governing the emergency plan and user notification.

13.11 Budgeting

a. Business Impact Analysis must be reviewed on regular basis in order for MLM IT Section to review its budgeting process.

b. It is the responsibility of the MLM IT Section to control the expenditures relating to the recovery and restoration effort.

13.12 Plan Activation

This section of an IT disaster recovery plan documents decision criteria used to activate the plan. Activation should occur when the damage assessment indicates one or more of the activation criteria for the system are met. The IT Disaster Recovery Team will activate the plan and the activation of the plan may be based on, but not limited to, the following:

a. Safety of personnel and/or extent of damage to the facility;
b. Extent of damage to a specific system or systems;
c. Ability to meet the agency's mission; and
d. Anticipated duration of disruption in relation to Recovery Time Objective (RTO)

13.13 Vital Records

a. All IT Systems equipment storing vital records should be recorded on the Disaster Recovery plan and stored in a single comprehensive database.
b. The MLM IT Data Backup policy must be implemented in determining what subset of backup data will be additionally encrypted, and stored off-site in a secured location.
c. Disaster Recovery Team and Municipal Manager must be granted authorisation to access a copy of emergency and recovery plan.

13.14 DR Plan Attributes

a. DR plans must address an outage that could potentially last for a period of up to six weeks.
b. DR plans must identify risk exposure and either accept the risk or propose mitigation solution(s).
c. Backup strategies must comply with predefined businesses continuity requirements, including defined recovery time and point objectives. Backup strategies must be reviewed annually.
d. Recovery strategies must meet recovery objectives defined in the DR tier chart.
e. Approved recovery strategies must be tested to ensure they meet required recovery time and recovery point objectives at least twice per annum. Such test must be documented and results of these tests kept for auditing and record purpose.
f. Recovery strategies must be implemented within a previously agreed upon period of time, generally not more than 180 days after management approval.
g. ITO or The Assist Director for IT is required to provide DR training and awareness activities to the Disaster Recovery Team at least twice per year.

13.15 Maintenance

a. MLM IT Section and Disaster Recovery Team shall ensure the accuracy of the information contained on the disaster recovery plan.
b. The backup system of vital data and information must be tested on regular basis and the warranty of the backup storage media must be monitored and any expired storage media shall be replaced and disposed.
c. The following maintenance activities must be conducted annually:

- Updating the documented Disaster Recovery plan
- Reviewing the Disaster Recovery Objectives and strategy
- Updating the internal and external contacts lists

- Conducting a simulation/desktop exercise
- Conducting a telecommunication exercise
- Conducting an application recovery test
- Verifying the alternate site technology
- Verifying the hardware platform requirements
- Submitting the Disaster Recovery Status and Recoverability Report

14. ELECTRONIC MAIL ACCEPTANCE USE POLICY

14.1 Overview

The email facilities are recognised as valuable tools to help Maruleng Local Municipality maintain an IT environment which efficiently supports core business and simplifies ease of access to information. However, the use of email carries some risk to users and MLM.

14.2 Purpose

This Policy sets out users and MLM's responsibilities and obligations in relation to electronic communication. This Policy emphasises that any use of email should reflect the same standards of professional conduct and ethics that are expected and maintained by Municipal users in other areas of their work.

14.3 Scope

This policy applies to all MLM users and to any other user(s) authorised to have access to the Municipal information systems.

14.4 Policy Statement

Email and other electronic data must be used primarily for business purposes, and in a manner, which does not risk damaging MLM's reputation and contributes to the safe, effective and accountable operation of Maruleng Local Municipality business.

Responsibility when using email lies with the individual user. It is the individual user who is accountable for any activity that does not comply with this Policy. This includes, but is not limited to any statement or use that breaches the law.

All material stored on electronic devices operated by MLM, or on MLM's behalf, is the property of MLM. This includes material stored on desktop computers or portable devices supplied by MLM, and material which may have been created for personal use, but has been stored on a MLM system and/or equipment.

14.5 Cautions

14.5.1 An email from a MLM IT equipment is effectively communication on behalf of MLM and may end up having a much wider distribution than intended. Communications by email must be courteous and professional. Employees should not say something in an email that they would not be comfortable putting in a letter or memorandum. It is inappropriate to send heated messages or exchanges by email.

14.5.2 MLM is subject to the Official Information Act therefore all emails received and sent may be required to be disclosed. All email messages sent with the MLM email address in the 'From:' or 'Reply To:' header, must be accompanied by the approved disclaimer to the effect that the views of the sender may not represent those of the MLM.

14.5.3 When sending an email to several people, a group should be set up in the email system and used. This prevents disclosure of personal email addresses and means that the members of the group will be protected from any virus that penetrates the security system and is aimed at addressees.

14.6 External Email Accounts and Instant Messaging

MLM IT section does not have control over the external email accounts like webmail, thus MLM cannot recommend the use of such email accounts because their confidentiality, integrity and availability cannot be assured. Therefore, MLM users are strictly prohibited to use these external email accounts to send, receive and store any official information and/or data unless authorised by MLM IT Section.

MLM IT Section strictly prohibit the use of Instant Messaging applications such as MSN, Yahoo messenger, etc. unless authorised by MLM because such applications are disposed to malicious code and can be used as entry points for viruses and worms into MLM's computer network.

14.7 Prevention of Malicious Software

All incoming emails and outgoing emails into and out of MLM computer network must be scanned in order to prevent computer malicious software (include viruses, computer worms and Spyware) from entering and infecting Municipal computer systems. The following will govern incoming and outgoing malicious or potentially harmful attachments:

- All virus infected mails will be blocked by default.
- All attachments that cannot be scanned for viruses will also be blocked.
- Typical virus hoaxes will be blocked.
- All executable files or documents with embedded executables will be blocked.

14.8 Communication of Official Information

MM will grant special authorisation to particular users to be responsible for distributing official information to both internal and external users.

14.9 Playful Use

MLM IT Section shall put in place technical measures to monitor and identify users who send mass mailings and distribute large files, music and video files and creating unnecessary loads of network related to personal use. Disciplinary measures shall be taken against such users.

14.10 Limitation of Privacy

MLM users should acknowledge and understand that email systems are there to improve information sharing and assist them in the performance of their jobs, therefore, there will be no privacy in anything they store or distribute using MLM email systems.

MLM IT Section will deploy strict technical measures in place to filter email content by automatically scanning all incoming and outgoing emails to ensure satisfactory email security and compliance to the policy. All non-compliant emails shall be blocked and the sender or receiver of the email will receive a notification clearly indicating why the email was blocked and he/she will be granted opportunity to request email release if the email content is business related.

14.11 Discriminatory, harassing and/or offensive language

MLM email systems shall not be a platform to exercise and promote the use of insulting, discriminatory or any offensive language. Necessary disciplinary actions shall be taken for users who will be caught using such language.

14.12 Monitoring and Reporting

MLM IT Section will continue to filter and monitor all incoming and outgoing emails traffic in order to establish if users do not spend most of their time sending personal emails rather than business emails. This will help the MLM IT Section to continuously improve email security and enforce compliance.

14.13 Access to another user's email

No MLM user shall have access to another user's email.

14.14 Automatic Forwarding of Emails

Since the confidentiality of external email addresses cannot be assured, MLM users are cautioned not to forward or create rules to automatically forward any official Emails to external email addresses in order to prevent sensitive official information from being disclosed.

14.15 Email Retention and Archiving

All MLM emails shall be archived by default on daily basis as part of MLM backup policy. The archives shall be backed up for a period of 5 years as per the National Archives of SA Act 43 of 1996

14.16 Dead, Chain Letters and Hoax and Spam Emails

Users must not use MLM Email systems to distribute chain letters, hoax and spam emails to other users. This is to ensure that Email resources are available to all legitimate users when necessary.

14.17 Prohibited Use

Prohibited uses of Email facilities include but are not limited to;

a. Distributing chain letters, junk mail and/or hoax email messages
b. Sending, receiving and storing of pornography and profanity
c. Sending, receiving and storing of audio and video files
d. Sending of emails to distribution lists to which you have not been granted the authorization
e. Sending of classified departmental information
f. Sending of emails of racial, hate, discrimination or sexist nature
g. Sending of unsolicited personal and commercial advertisements or promotions to other staff members or external email recipients
h. Sending of other people's confidential and personal information
i. Sending of data that violates copyright laws
j. Use of electronic mail to harass or intimidate others or to interfere with or deny other legitimate users the ability to effectively carryout their official duties
k. Use of electronic mail in any manner prohibited by national and international laws and regulations
l. "Email Spoofing" i.e. constructing emails so it appears to be from someone else
m. "Snooping" i.e. obtaining access to other people's emails for the purpose of satisfying curiosity
n. Attempting unauthorised access to electronic emails or attempting to breach security systems of any email system or "eavesdropping" i.e. attempting to intercept any electronic mail transactions without proper authorisation

14.18 Disclaimer

All email messages sent from MLM's email systems will automatically be stamped with the following disclaimer:

"The contents of this e-mail and any attachments are confidential. It is intended for the named recipient(s) only. If you have received this email in error please notify the sender immediately and do not disclose the contents to any one or make copies. Please note that the recipient must scan this e-mail and any attached files for viruses and the like. While we do everything possible to protect information from viruses, MLM accepts no liability of whatever nature for any loss, liability, damage or expense resulting directly or indirectly from the access and/or downloading of any files which are attached to this e-mail message. Opinions, conclusions and other information in this message that do not relate to the official business of MLM be understood as neither given nor endorsed."

14.19 Authorisation Procedures

14.19.1 Application of Email Access

New email addresses shall be created for the user upon completion and signing of the undertaking Form to be issued by the MLM IT Section and such signed Form shall be filed in the user's file.

14.19.2 Email User's Responsibilities

Email users have the following responsibilities:

a. Ensure that their usernames and passwords are kept secure and not shared
b. Fully comply with all aspects of this policy
c. Immediately alert IT Section (Information Security/Incident Response) about any misuse and non-compliance.
d. Not to waste computer/network resources
e. Continuously protect the integrity and public image of MLM

14.19.3 IT Section Responsibilities

a. Implement technical measures to ensure adequate Confidentiality, Availability and Integrity of MLM email systems.
b. Monitor and enforce policy compliance.
c. Follow appropriate channels to resolve policy breaches and incidents.
d. Educate Emails users whenever possible about Email security best practices and this Electronic Mail Acceptable Use Policy.

15. PROTECTION OF PERSONAL INFORMATION (POPI)

15.1 Overview

The preamble to POPI records that POPI emanates from section 14 of the Constitution of the Republic of South Africa, 1996, which section provides that everyone has the right to privacy and it includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.

POPI gives expression to the constitutional values of democracy and openness, recognising the need for economic and social progress within the framework of the information society and the need for a removal of unnecessary impediments to the free flow of information, including personal information.

POPI has been promulgated to regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests.

15.2. Purpose

The primary purpose of this policy is to provide information with regards to requirements and guidelines of processing and storing personal information for data subjects who includes applicants and former job applicants (successful or unsuccessful), former or current employees, temporary employment services staff, casual staff, staff on secondment and those on work experience placements.

MLM will ensure that each employee adheres to the guidelines of this policy and performs their duties in accordance with the policy and procedures of the POPI Act.

This document will serve as a tool in regulating the primary functionalities of balancing the right to privacy and the right to access of information. It will also serve as a guideline on how personal information should be stored and processed.

15.3. Scope

This policy is applicable to all Employees of MLM, including all applicants and former job applicants (successful or unsuccessful), former or current employees, temporary employment services staff, casual staff, staff on secondment and those on work experience placements, contractors, suppliers, and any persons acting on behalf of the MLM.

All of the abovementioned personnel are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.

15.4 Policy Statement

This policy also serves to protect Maruleng Local Municipality from compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality
- Failing to offer choice to Data subjects to choose how and for what purpose their information is used
- Reputational damage.

This policy also demonstrates the MLM's commitment to protecting the privacy rights of Data subjects.

15.5 Rights of Data Subjects

A Data subject has the right to have their personal information processed in accordance with their special conditions for lawful processing which includes the right to:

a. Being notified when their personal information is collected and when it has been accessed or acquired by an unauthorised person.
b. To request access to their personal information.
c. To request, where necessary, the correction, destruction, or deletion of their personal information.
d. To object to the processing of their personal information being used for direct marketing by means of unsolicited electronic communications.
e. To not be subject, under certain circumstance, to a decision which is solely based on the automated processing of their personal information intended to provide a profile of such person.
f. To submit a complaint to the Regulator regarding the alleged interference with the protection of their personal information or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in the Act.
g. To institute civil proceedings regarding the alleged interference with the protection of their personal information.

Should an employee of MLM be requested access to their personal information, such request should be made on a Personal Information Request Form.

15.6. Conditions for Lawful Processing of Personal Information

All employees and persons acting on behalf of MLM will always be subject to, and act in accordance with, the following guiding principles:

15.6.1 Accountability

15.6.1.1 MLM' employees are to ensure that personal information is lawfully processed in accordance with POPI Act at all times.
15.6.1.2 MLM is required to audit the processes used to collect, record, store, disseminate and destroy personal information.
15.6.1.3 MLM is to ensure the integrity and safekeeping of personal information that is in its possession or under its control.
15.6.1.4 MLM is to ensure uncompromisable data security system in order to prevent data subject's information from being lost, damaged, or unlawfully accessed.

15.6.1.5 All employees of MLM must ensure that all processing conditions under this heading are complied with when determining the purpose and means of processing Personal Information.

15.6.2. Processing Limitation

15.6.2.1 Lawfulness of processing:

a. Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.
b. Processing is deemed to be lawful only if the information being processed is obtained adequately, and that it is relevant and not excessive.
c. Personal Information may only be processed by MLM if it meets one of the following lawful processing standards:

    i. The Data Subject is aware and consents to the processing.
    ii. Processing is necessary for the conclusion of any contract or transaction with the Data Subject.
    iii. Processing complies with a legal responsibility imposed on MLM.
    iv. Processing protects a legitimate interest of the Data Subject.
    v. Processing is necessary for fulfilment of a legitimate interest of MLM or correspondent attorneys to whom the information is supplied to.

15.6.2.2 Special Personal Information includes:

a. Religious, philosophical, or political beliefs.
b. Race or ethnic origin.
c. Trade union membership.
d. Health or sex life.
e. Biometric information (including but not limited to blood type, fingerprints, DNA, retinal scanning, voice recognitions, photographs).
f. Criminal behaviour.
g. Information concerning a child.

15.6.2.3 MLM may only process Special Personal Information under the following circumstances:

a. The Data Subject has consented to such processing.
b. The Special Personal Information was deliberately made public by the Data Subject.
c. Processing is necessary for the establishment of a right or defense in law.
d. Processing is for historical, statistical or research reasons; and / or
e. If the processing of race or ethnic origin, is to comply with the affirmative action laws.

15.6.2.4 All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object at any

time, to the processing of their Personal Information, unless legislation provides for such processing. If the Data Subject withdraws consent or objects to processing, then MLM shall immediately refrain from processing the Personal Information.

15.6.3. Purpose Specification

15.6.3.1 Personal Information must be collected for a specific, explicitly defined, and lawful purpose related to a function or activity that MLM renders.

15.6.3.2 MLM is to ensure that the Data Subjects are made aware of the purpose for which the collection of their Personal Information is for.

15.6.3.3 The purposes for collecting Personal Information must relate to the following:

a. Administration of agreements.
b. Providing products and services to clients.
c. Detecting and prevention of fraud, crime, money laundering and other malpractices (FICA).
d. Conducting market and/customer satisfaction research.
e. Marketing and sales.
f. In connection with any legal proceedings.
g. Staff administration.
h. Keeping of accounts and records.
i. Complying with legal and regulatory requirements.
j. Obtaining Personal Information for bond registrations and transfers of properties; and / or
k. Profiling data subjects for the purposes of direct marketing.

15.6.3.4 Retention and Restriction of Records:

a. Personal Information must not be kept longer than is necessary for achieving the purpose for which the information was collected or subsequently processed.
b. MLM must destroy or delete a record of personal information as soon as MLM is no longer authorised to retain the record.
c. MLM must ensure that the destruction or deletion of Personal Information must be done in a manner that prevents its reconstruction in an intelligible form.

15.6.4 Further Processing Limitation

15.6.4.1 Further processing of Personal Information must be in accordance with the specific purpose for which it was collected.

15.6.4.2 To assess if further processing is line with the purpose collected for, MLM must consider the following:

a. The relationship between the purpose of the intended further processing and the purpose for which the information has been collected.
b. The nature of the information concerned.
c. The consequences of the intended further processing for the data subject.

d. The nature/system in which the information has been collected.
e. Any contractual rights and obligations between the parties.

15.6.4.3 Further processing of Personal Information is not in accordance with the purpose of collection if:

a. Where the Data Subject is a child has consented to the further processing of the information.
b. The information is available in or derived from a public record or has been deliberately made public by the data subject.

15.6.4.4 Further processing is necessary in the following instances:

a. To avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution, and punishment of offences.
b. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue.
c. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
d. Is the interest of national security.

15.6.5 Information Quality

15.6.5.1 MLM must take reasonable steps to ensure that the Personal Information obtained from Data Subjects is complete, accurate, not misleading and updated where necessary, and that the information is collected in regard to the purpose.

15.6.5.2 Employees should by all means follow the following guidance when collection Personal Information:

a. Personal Information should be correctly dated and marked when received.
b. A record should be kept of where the Personal Information was obtained from.
c. Changes to information records should be dated and signed.
d. Irrelevant or unneeded Personal Information should be deleted or destroyed.
e. Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system or both.

15.6.6 Openness

15.6.6.1 Documentation

a. Employees must maintain the documentation of all processing operations under its responsibility as referred under retention and restriction of records.
b. MLM employees must take reasonable practical steps to ensure that the Data Subjects are aware of:

- The reason for which information is being collected and where the information is not collected from the data subject, the source from which it is collected.
- The name and address of the MLM.
- The purpose for which the information is being collected.
- Whether or not the supply of the information by that data subject is voluntary or mandatory.
- The consequences of failure to provide the information.
- Any law authorising or requiring the collection of the information.
- The fact that, where applicable, the MLM intends to share the information to a third party or international organisation and the level of protection afforded to the information by that third party or international organisation.
- That the Data Subject has the right to access or rectify the information collected.
- That the Data Subject has the right to object to the processing of their Personal Information; and
- MLM has the obligation to inform the Data Subject that should they be unhappy in the way their Personal Information is being processed or stored that they have the right to lodge a complaint to the Information Regulator.

15.6.7 Security Safeguards

15.6.7.1 MLM must ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

a. Identify all reasonably foreseeable risks to information security.
b. Implementing security controls to minimize the risk of loss, unauthorised access, disclosure, interference, modification, or destruction.
c. Security controls implemented should be context sensitive. This meaning that the more sensitive personal information is – the greater security is required.

15.6.7.2 Written records:

a. Personable Information records should be kept in areas that non-staff members have access to.
b. When in use, Personal Information records should not be left unattended in areas where non-staff members may access to.
c. MLM shall implement and maintain a “Clean Desk Policy” where all employees shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day.
d. Personal Information which is no longer required should be disposed by shredding.
e. All FICA documents must be uploaded onto MLM’ online portal and the hard copies must be stored away in a designated secure storage unit.
f. Any loss, theft or unauthorised access to Personal Information must be immediately reported to the Information Officer.

15.6.7.3 Electronic Records:

a. All electronically held Personal Information must be saved on an online portal.
b. As far as reasonably practical, no Personal Information should be saved on individual computers, laptops, or hand-held devices.
c. All computers, laptops and hand-held devices should be access protected with a password, fingerprint, retina scan or facial recognition, with the password being of reasonable complexity and changed monthly.
d. MLM shall implement a "Clean Screen Policy" where all employees shall be required to lock their computes or laptops when leaving their desks for any length of time and to log off at the end of each day.
e. Electronic Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employees must ensure that the information has been completely deleted and is not recoverable.
f. Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer who shall notify the IT Department who will then take all the necessary steps to remotely delete the information, if possible.
g. MLM will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyberattacks on the IT network.

15.6.8 Data Subject Participation

15.6.8.1 Data Subjects have the right to request access to their Personal Information.

15.6.8.2 Data Subjects have the right to request for their Personal Information to be amended or deleted.

15.6.8.3 All of the above requests stipulated in 5.8.1 and 5.8.2 must be submitted in writing to the Information Officer, unless there are grounds for refusal as set out in below, MLM shall disclose the requested Personal Information:

a. On receipt of satisfactory proof of identity from the Data Subject or requestor.
b. Within a reasonable time.
c. On receipt of the prescribed fee, if any.
d. In a reasonable format.

Personal Information shall not be disclosed to any party unless the identity of the requestor has been identified.

15.7 General Description of Information Security Measures

MLM deploys up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its case. These measures include:

a. Firewalls.
b. Virus protection software and updated protocols.
c. Logical and physical access control.

d. Secure setup of hardware and software making up the IT infrastructure.
e. SETA and Outsourced Service Providers who process Personal Information on behalf of MLM are contracted to implement security controls.

15.8 Access to Personal Information

15.8.1 Any requests to access, amend or delete Data Subject's own Personal Information held by MLM, should be directed on the prescribed form to the Information Officer.

15.8.2 Remedies available if request for access to Personal Information is refused:

Internal Remedies: The Act does not provide any internal remedies should a request for Personal Information is made and is denied by the Information Officer. However, should a requestor or third party be dissatisfied with the Information Officer's refusal to disclose information, may withing 10 working days of notification of the decision escalate the matter to the MLM HR Manager who will engage the MLM MM in order to make a decision.

External Remedies: Should a requestor or third party be dissatisfied with the Information Officer's refusal entire internal remedies process to disclose information, may within 30 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court, or another court of similar status.

15.8.3 An Information Officer may refuse the request to Personal Information on the following grounds:

a. Protecting Personal Information that MLM holds about a third party (who is a natural person) including a deceased person, from unreasonable disclosure.
b. Protecting commercial information that MLM holds about a third party that could harm the integrity or financial interest of the organisation or the third party.
c. If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement.
d. If disclosure of the record would endanger the life or physical safety of an individual.
e. If disclosure of the record would prejudice or impair the security or property or means of transport.
f. If disclosure of the record would prejudice or impart the protection of the safety of the public.
g. The record is privileged from production in legal proceedings unless the legal privilege has been waived.
h. Disclosure of the record that would put MLM at a disadvantage in contractual or other negotiations or prejudice it in commercial competition.
i. The record is a computer programme, and contains information about research being carried out or about to be carried out on behalf of a third party or MLM

15.8.4 Records that cannot be found or do not exist:

Should a Data Subject request MLM to search for a record and it is believed that the record does not exist or cannot be found, the requestor must be notified by way of affidavit or affirmation. Steps that were taken to try locating this record must be stated on the affidavit/affirmation.

15.9 Implementation Guidelines

15.9.1 Training and Dissemination of Information

a. Training on the Policy and POPI will take place with all affected employees in MLM.
b. All new employees will be made aware of this policy or through training programmes of their responsibilities under the terms of this Policy and POPI.
c. Modifications and updates to data protection and information sharing policies, legislation or guidelines will be brought to the attention of all staff.

15.9.2 Employee Contracts

15.9.2.1 Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information and a confidentiality undertaking that the employee will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information that the employee deals with or oversees, however it is stored. Failure to comply will result in the necessary disciplinary action being taken against the contravening employee.

15.9.2.2 Each employee who is currently employed with MLM will sign an addendum to their Employment Contact containing the relevant consent clauses for the use and storage of employee information and a confidentiality undertaking that the employee will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information that the employee deals with or is in charge of, however it is stored. Failure to comply will result in the necessary disciplinary action being taken against the contravening employee.

15.10 Direct Marketing

15.10.1 All Direct Marketing communications shall contain MLM details and an address or method for the customer to opt-out of receiving further marketing communication.

15.10.2 Existing Clients:

a. Direct Marketing by electronic means to existing clients is only permitted:
    - If the client's details were obtained in the context of a service; and
    - For the purpose of marketing similar products or content.
b. The client must be given the opportunity to opt-out of receiving direct marketing on each occasion of direct marketing.

15.10.3 Consent

MLM may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. MLM may approach a Data Subject for sent only once.

15.10.4 Record Keeping

MLM shall keep record of:

a. Date of consent.
b. Wording of the consent.
c. Who obtained the consent?
d. Proof of opportunity to opt-out on each marketing contact.
e. Record of opt-outs.

15.11 Information Officer

15.11.1 MLM will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

15.11.2 The Information Officer is responsible for ensuring compliance with POPI Act.

15.11.3 MLM may annually consider a change in the Information Officer and Deputy Officer.

15.11.4 The Information Officer will be issued with Guidance Notes on their duties and same can be accessed on request to the Information Officer.

15.11.5 The Information Officer is to attend to any complaints issued to him/her on the prescribed form

15.12 Information Technology

15.12.1 Ensuring that the IT infrastructure, electronic filing system and any other devise used for processing personal information meet acceptable security standards.

15.12.2 Ensuring that all electronically held personal information is kept only on designated drives and serves and are u-loaded only to approved cloud computing services.

15.12.3 Ensuring that all servers containing personal information are stored in a secure location, away from the general office space.

15.12.4 Ensuring that all back-ups containing personal information are protected from unauthorised access and malicious hacking attempts.

15.12.5 Ensuring that personal information being transmitted electronically is encrypted.

15.12.6 Performing regular IT audits to ensure that the security of the firm's hardware and software systems are functioning.

15.12.7 Performing regular IT audits to verify whether electronically stored personal information has been access or acquired by any unauthorised persons.

15.13 Employees and Other Persons Acting on Behalf of MLM

15.13.1 All employees and other persons acting on behalf of MLM will, during the course of the scope and duties of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

15.13.2 Employees and other persons acting on behalf of MLM are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

15.13.3 Employees and other persons acting on behalf of MLM may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the Municipality or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

15.13.4 Employees and other persons acting on behalf of MLM must request assistance from the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

15.13.5 Employees and other persons acting on behalf of MLM must always adhere to the 8 processing conditions of personal information and must always obtain consent from the Data Subject before processing / using or storing their Personal Information.

15.14 Destruction of Documents

15.14.1 Documents may be destroyed after the termination of the retention period as determined by MLM from time to time.

15.14.2 Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on regular basis. Files must be checked to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by MLM pending such return.

15.14.3 The documents must be shredded or use of another approved document disposal company.

15.14.4 Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

16. PROCEDURE MANUALS

16.1 Managing IT Issues

a. All IT related issues shall be addressed to the IT Section by logging an IT Call.
b. No user shall try and fix any IT issues encountered. All IT issues to be reported to IT Section, irrespective of the nature of the issue.
c. Users will only be allowed to diagnose their IT equipment before logging a Call to IT Section. The diagnose process shall strictly be conducted as follows (in the order they appear):

    1. All cable Connections
    2. All peripheral connections
    3. Power connections
    4. Reboot if possible (Switch off the plug on the wall socket)

16.2 Logging an IT Call

MLM users shall adhere to the following steps when logging an IT Call:

a. User shall complete IT Call Logging Register Form and state the nature of the issue.
b. Completed IT Call Logging Register Form shall be emailed or hand delivered to the IT Section using the designated IT Call Logging Email Address.
c. An automatic “nonreply” email shall be sent back to the user to acknowledge receipt of the IT Call and alert the user that they will receive reference number with the name of the IT Official assigned to the call.
d. The IT Section shall assess the level of priority and urgency to the issue(s) and allocate turnaround time.
e. Once the assessment is done, a reference number will be generated and the call assigned to the IT Official.
f. Both the IT Call Reference Number and the name of an IT Official assigned to the Call shall be emailed to the user.
g. The IT Official assigned to the issue shall liaise with the user throughout the process of working on the issue.
h. IT Official shall advise the user if the issue(s) was/were fixed. If fixed, the user shall test the IT equipment or system and advise the IT Official to close the Call. If not fixed, the user shall advise the IT Official who will initiate investigations and escalate where necessary.
i. An IT Call shall be closed only when the issue(s) is/are fixed and the user is happy about the outcome.

16.3 Managing Anti-Virus(es)

Maruleng Local Municipality Anti-Virus(es) will be managed centrally and will be set to run in the background, automatically download updates and auto-install them without interfering and distracting users in their daily operations. This auto download and update will take effect once the IT equipment is connected to the MLM network on daily basis.

16.4 End-User

16.4.1 Network & PC Storage

All MLM data files and emails shall be saved in the network folders.

16.4.1.1 Saving Files (First time only)

The MLM IT Systems shall deploy standardized Microsoft® Windows® Professional 64-bit and Microsoft® Office 64-bit across the Municipality.

The following process shall be followed when saving files for the first time in Microsoft Office Applications such as MS Word, Excel, Power point, Access, Projects, etc.:

a. Click the "File" in the menu bar or click the "Save" icon in the standard bar.
b. Click 'Save' (a "Save as" message box will appear),
c. Make sure of the location is either my documents or your external storage (A drive) and name the file appropriately,
d. Click the "Save" button.
e. Alternatively, replace step (a) with Ctrl-S with in the Microsoft® application.

16.4.1.2 Resaving files

a. Click "file", "Save"
b. Click the "Save" button in the standard menu bar or
c. Alternative replace step (a.) with Ctrl-S within the Microsoft® application.

16.4.1.3 Resaving Files (with a different name)

a. Click "File",
b. Click "Save As"
c. Click the "Save AS "message box, change the file name
d. Click the "Save Button"

16.4.1.4 Open Saved File

a. Click File,
b. Click Open,
c. Select the Saved File, and
d. Double Click the File.
e. Alternatively replace step (a.) and (b.) with Ctrl-O

16.4.1.5 Print

a. Click File
b. Click Print
c. Alternative replace step (a.) with Ctrl-P

16.4.1.6 Deleting Files

a. Deleting Network Files:

The deletion of network files from the MLM network shall be authorised by the Municipal Manager and IT Section in order to prevent the deletion of files and data which is still valuable to the Municipality and its operations because the deletion of network files is permanent and can only be restored if they were backed up and the backup is not wiped out.

b. Deleting PC Files:

The deletion of PC files does not require authorisation; however, it is the responsibility of the user to assess the files and data before deleting them. The following process shall be followed when deleting PC files:

a. Double-click the “My Computer” button
b. Navigate to the folder where the file to be deleted is located,
c. Click the file once only (it will be highlighted / selected),
d. Press the “Delete “button on the keyboard,
e. Confirm deletion by clicking the “Yes” in the confirmation window.

NB:
Selecting Number of Files:

- Press and hold “ctrl” button and click on files you want to select one by one until they are all selected, then release the button. Or click on one file you want to delete, press and hold “shift” button and click on the last file to be selected.

16.4.2 Managing Electronic Mails

16.4.2.1 Creating New Email

a. Open Microsoft Outlook application,
b. Click the “New” icon-a blank window for new mail will appear,
c. Enter the correct destination e-mail address,
d. Enter the correct Heading / Subject for your correspondence,
e. Attach a file in necessary (see point to below on how)
f. Click the “send” button.

16.4.2.2 Deleting Email in Inbox or Sent Mails

a. Inside the e-mail application “Outlook,
b. Click the folder on the right-hand column,
c. Right click the mail item to be deleted,
d. Select Delete, or
e. Alternatively –select the mail item and press the delete button.

16.4.2.3 Deleting Email from Deleted Mails

a. Make sure that a correct folder is selected e.g. Deleted Items
b. Select the file to be deleted on the right-hand column and press delete key on the keyboard.
c. If the deletion is made from any folder than the Deleted Items”, files will be deleted without any message box popping for confirmations. Files are placed in the “””,
d. If the deletion is made from Deleted Items, a message dialog box will pop up requiring confirmation of deletion of emails. This deletion is permanent and can only be restored if backup of such email was retained prior to deletion. Emails and all its attachments will be removed from the folder.

16.4.2.4 Attaching Files

There are three ways of attaching files from an external source into an e-mail message. These are three ways:

From within Outlook Application

a. Make sure that the cursor is at the right location
b. Click the “Attach File” icon on the menu ribbon. A dialog box “Insert File” will appear
c. Navigate to correct location and click file to be attached.
d. Click the Insert button. This will take you back to Outlook with the file attached.
e. Continue as usual

Inside a Windows application

Without having opened Outlook, the action defined below will open a new e-mail message window with the attachments(s) already inserted Inside the Microsoft Application (e.g. MS Word), with the document already typed;

a. Click File,
b. Clicks Send To,
c. Click Mail Recipient (As Attachment).

A new email message dialog box with the file already attached will open up. Just fill in the other fields, type message, and proceed as usual. From Any Folder e.g. Desktop, C:\, H:\

a. Navigate to the folder that contains the file (s) to be attached,
b. Right click the files and select send to
c. Click mail recipient
d. A new e-mail message with the attachments will be open. Just fill in the other fields, type message, and proceed as usual.

16.4.2.5 Opening Attachment Files

Attachments will generally be part of the email message header at the top of e-mail window. It does happen however, that an attachment be located inside the message box or at the bottom of the of the email window, especially when access via web interface.

a. In Outlook, with the email windows open, double click the attached file to pen it.
b. If the attached file has no default application associated with it installed, a user may be required to select appropriate application/program to use to open the attachment.
c. Outlook may at times ask a user if they want to open or save the file. Select the appropriate option and follow the usual process

NB: Windows will generally automatically detect the type of the file and open it using the right application.

16.4.2.6 Creating E-mail Folders

Creating folders in Outlook is similar to creating folder in the “Windows Explorer”. Please note that there are sub-folders with folders. The main folder contains a “+” sign indicating

that there are sub-folders in that folder. The "- "sign indicates that the subfolders within a folder have been opened.

a. Right click the folder in which you want to create a sub-folder,
b. Click on "New Folder",
c. Enter the appropriate name for the folder to be created,
d. Click the "OK" button,
e. The folder will appear back in Outlook.

16.4.2.7 Moving Mail

Folders can be created to organize mail storage. Archive folders are created to facilitate organization of mail files. These folders are created outside Outlook – in the home directory folders (to lessen storage burden on the mail serve).

Once the archive folder is in place, the following procedure is followed: -

a. Note the folder marked 'Personal Folders' and all its contents,
b. Select the mail files(s) to be moved from the right-hand column,
c. Press and hold the left button of the mouse and drag the selected items to the desired folder (into the right-hand column) in the folder marked
d. Personal "Folders" Selected items will be moved

16.4.2.8 Archiving

This action will frequently be conducted by all staff for purposes of saving their mail for longer periods as the email storage quotas are reached. This action lessens the storage requirement and processing workload on the Mail Server in that all archive storage's take place on the File Server instead of the Mail Server.

17. Conclusion

17.1. Implementation

This policy comes into effect from the date of approval.

17.2. Enforcement

Municipal Manager is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

17.3. Consequences of Non-Compliance

Anyone found to be in violation of this policy may be subject to MLM disciplinary code

17.4. Policy Review

This policy shall be reviewed annually.

17.5. Approval and Adoption

Approved by:

_____ _____

Ms Hoaeane NS (Municipal Manager) Date

ANNEXURE A: IT CALL LOGGING REGISTER

Reference number/Day/Month/year	Call Logged By	User's Contact and location	Nature of the Call	Date Call Logged	Date Call Resolved	Call logged Assigned To	Cal llogged Output	IT Manager Signature

ANNEXTURE B: USER ACCOUNT CREATION AND PASSWORD RESET FORM

User Information

Surname: …….. Initials: ……

Network Username: ……

Employee Number: …….. ID Number: ……

Directorate: …… Division: ……

Contact\Tel\Ext Number: ……

User account creation ☐ **Password reset** ☐

User account or Password reset for

Domain Account		Munsoft System Account		Sage 300 Account		Other account(specify)	

Mark X in the box

Reason for Password Reset		**Reason for account creation**	
Password Forgotten		Newly appointed	
Password Expired		Transferred	
Password blocked		External support	
Suspected Breach/Disclosure		Others	

More Details……

Acknowledgement and Authorization

I hereby request IT Official to reset my password and I declare that all the details on this form are correct and do not contain any other individual's details other than my own. I agree to safeguard my user account and password details in accordance to the Information Technology policies.

Name: ……

Signature: …… Date: …… Time: ……

For IT Office Use Only

Password Reset By: ……

System/Application/Resource: ……

Signature: …… Date: …… Time: ……

ANNEXTURE C: IT ASSET RELEASE FORM (ITARF)

NOTIFICATION FOR REMOVAL / TRANSFER OF IT ASSETS

[This form must be utilized as the only standard document for the movement of IT assets. To be completed and signed by computer users when transfers of assets occur between locations and between users, and during the resignation of personnel]

FROM:		TO:	
Employee (User)		Employee (User)	
Office & Building		Office & Building	
Telephone Number		Telephone Number	
Division & Directorate		Division & Directorate	

Category (e.g., CPU)	Make (e.g., Mercer)	Model (e.g., Premium X)	Serial no (By manufacturer)	MLM Asset no (Permanent marker no)

Transfer of the above listed IT assets between employees / users

Released (Signed off) by: …… Date: …….

Received by: …… Date: …….

For updating of the above records on the IT asset register, please submit this to the IT Office

FOR USE BY ITO ONLY

The Asset Register has been updated YES/NO ☐ ☐

Date: ……

Name in print: …… **Signature:** ……

ANNEXTURE D – CHANGE MANAGEMENT FORM

CHANGE MANAGEMENT FORM

GENERAL INFORMATION:

SERVER NAME (where upgrade is to done)	APPLICATION NAME (e.g. VIP, Munsoft etc.)

TYPE OF CHANGES:

Upgrade	

BRIEF DESCRIPTION OF CHANGE

AUTHORISATION OF CHANGE: CFO/ICT MANAGER/MUNICIPAL MANAGER:

Name		Dept		Signature		Date	

WORK PERFORMED BY:

Service Provider		ICT Manager		Both	

CHANGES CHECKED AND VERIFIED BY:

Name		Dept		Signature		Date	

ANNEXTURE E – IT USER REQUEST FORM

User Information

Surname: …….. Initials: ……

Employee Number: …….. ID Number: ……..

Contact\Tel\Ext Number: ……

Incident description(Low 4hrs to 8hrs, Medium 2hrs to 4hrs, High 0 to 2hrs)

IT Issue description	Low Priority	Medium Priority	High Priority

Call assigned to ……Signature……..

ITO Report (Tick box with X)

Issue resolved		Escalated		Other	

More Details……

……

Client rating (X)

Own Rating	1- Not satisfactory	2- Less Satisfactory	3- Satisfactory	4- More satisfactory	5- Very Satisfactory

Name……..

Signature…….. Date…….. Time……

_____For IT Office Use Only_____

Call attended by……

Signature…….. Date…….. Time……

ANNEXTURE F: <u>OFFICIAL WEB CONTENT UPDATES SCHEDULE</u>

NAME OF DOCUMENT	TYPE OF DOCUMENT	SOURCE DIRECTORATE	RESONSIBLE OFFICIAL	REMOVAL DATE AND TIME	SUBMISSION DATE AND TIME	PUBLISHING DATE AND TIME	COMMENTS