MOPANI DISTRICT MUNICIPALITY

INFORMATION TECHNOLOGY

POLICIES, GUIDELINES, AND PROCEDURES

Version: 1.3.4

TABLE OF CONTENTS

VERSION CONTROL

Version	Date	Author(s)	Details
Draft 1.0	2012/02/10	Rasekgala MJ	First Draft
Draft 1.1	2012/02/02	Rasekgala MJ	Changes to Table of Definitions of Terms and Abbreviations
Draft 1.2	2012/12/14	Rasekgala MJ	Consolidations of all IT Policies, Procedures and Guidelines into single document.
Draft 1.2.1	2013/01/11	Rasekgala MJ	Inclusion of Table of Contents
Draft 1.3	2013/03/20	Rasekgala MJ	Inclusion of Web Content Management and IT Disaster Management Policies
Draft 1.3.1	2013/03/22	Rasekgala MJ	Grammar and Spelling Corrections
Draft 1.3.2	2013/10/21	Rasekgala MJ	Insert Password Reset Request Form. Change Annexure Chapters and page numbers to merge new form explained above.
Draft 1.3.3	2016/01/04	Rasekgala MJ	Inclusion of the Password Reset Request Form
Draft 1.3.4	2024/05/02	Ngobeni EN	Changes on Specifications and operating system.

REFERENCES

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

- The Constitution of the SA, Act 108 of 1996
- Municipal Finance Management Act 1 of 2004
- Local Government Municipal Structure 117 Act 0f 1998
- Local Government Municipal Systems Act 32 of 2000
- Mopani District Municipality Supply Chain Management Policy
- 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.
- The State Information Technology Agency (SITA) Act, as amended.
- Electronic Communication Transaction Act.
- The protection of Information 84 Act of 1982
- The promotion of Access to Information Act
- The National Archives Act 43 of 1996
- Information Security Policy: Securing Information in the digital Age (Draft)
- Fire brigade Act 99 of 1987
- Copyright Act 98 of 1978
- Local Government Municipal Systems Act 32 of 2000
- opani District Municipality Supply Chain Management Policy
- 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.
- The State Information Technology Agency (SITA) Act, as amended.
- Electronic Communication Transaction Act.
- The protection of Information 84 Act of 1982
- The promotion of Access to Information Act
- The National Archives Act 43 of 1996
- Information Security Policy: Securing Information in the digital Age (Draft)
- Fire brigade Act 99 of 1987
- Copyright Act 98 of 1978

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	Authorisation 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.
Cascading	Cascading is the term often given to the movement of PCs within an organisation
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.
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.
EMT	Emergency Management Team, an MDM 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
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 authorised entry to the Municipality's resources such as workstations, networks and applications. Identification is closely linked to authentication
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 clients 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 ICT Officers.
MDM	Mopani District Municipality
MM	Municipal Manager

Municipality	Mopani District 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 **MDM** to personnel for business activities and official use.
Personnel	includes employees/staff/officials employed permanently and temporarily as well as supplied by labour brokers or service-providers
Prescripts	Regulations, instructions and directions.
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.
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.
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 authorisation 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)	Authorised individual(s), making use of the Municipality IT Infrastructure
WWW	World Wide Web, a system of interlinked hypertext documents accessed via the Internet.

Where reference is made to one gender in this policy it also includes and refers to the other gender.

1. PREAMBLE

In the 21st century and the Information Age, a combination of dramatic sociological, political, economic and technological factors is at play to bring about fundamental and irreversible changes in the entire social system. The scope of these transformations is global. In the times to come, economic power of nations is going to be a function of information technology (IT).

Recent technological advancements, like the Internet, have digitally broken the geographical, physical, political and even sociological boundaries transforming the world to a 'Global Village'. Even though all countries, and indeed organisations, shall be competing on a common denominator, its success would be determined by inputs from and to the information technology industry.

Information Technology has emerged as the single most important enabler for improving efficiency and effectiveness of organizations. Recognizing the enormous potential of IT, Mopani District Municipality should 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.

It is the intention of the Mopani District Municipality to consolidate its efforts and to focus its energies to leverage the potential of IT for the benefit of its people. With a view of attaining this objective, a comprehensive 'IT Policy' of Mopani District Municipality has been prepared.

In order for effective governance to be in place, the goals of the IT unit and the goals of the municipality must be clearly tied together. Too often, a very casual relationship exists between the two or none exists at all. When this occurs, IT initiatives crop up that have no bearing on the strategic goals of the municipality. When this happens, both the municipality and IT resource begin to wonder why a specific project is even being deployed.

The Information Systems Strategic Plan (SISP), also referred to as the Master Systems Plan (MSP) document attempts to develop a formal and direct link between information technology resources and strategic goals of the municipality. It is through this SISP/MSP that IT Governance of IT was identified as a critical factor in alignment of MDM strategic goals and its information technology for maximum and successful leverage of IT. As a result, The IT Governance Framework was developed and submitted for considerations and adoption by management.

The IT Governance Framework clearly defines all the necessary guidelines, standards, structures, policies, and procedures, etc. that are necessary for ensuring good governance of information technology. This document sets out these 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 ASSET MANAGEMENT POLICY

2.1 INTRODUCTION

Information Technology assets and equipment are a crucial element to every business environment. They provide for efficiency in day-to-day tasks and the communication needs of an organization. Despite their usefulness, IT assets can expose the Municipality to several risks. This policy on the use of IT Assets aims to provide for effective control, management and maintenance of the IT equipment.

2.2 BACKGROUND

In accordance with the Municipal Structures Act and the Municipal Finances Management Act, Mopani District Municipality has assigned the Corporate Services Directorate the following duties: Develop and adopt policies, standards, and guidelines for managing Information Technology. It is for this reason, together with the recommendations of the Auditor General and the Internal Audit Unit and guidelines from best practice standards and governance frameworks such as King III Report of Corporate Governance and **CoBIT**, that ITO has developed this policy that describes the methods for proper acquisition, installation, handling, tracking and disposal of IT assets to meet defined requirements. These IT asset management requirements include ensuring adherence to Municipality and industry standards, ensuring consistency throughout the Municipality, and conforming to User, Legal, and Regulatory requirements.

2.3 PURPOSE

The purpose of this policy is to regulate usage of IT Assets so that the Municipality:

- effectively controls the economic interest of computer software and hardware resources;
- reduces total cost of ownership (TCO);
- increases the return on IT infrastructure investment;
- maintains an accurate and current inventory of the Municipality's IT assets;
- encourages proper and efficient use of **MDM** IT assets;
- minimizes loss of, and damage to, computer equipment, software and data;
- is protected from possible legal difficulties due to computer usage;
- is productive, by limiting personal use to reasonable levels;

2.4 SCOPE OF THE POLICY

This policy is applicable to all permanent, contract and temporary personnel employed by the **MDM** who have been issued with a Municipality computer. In this policy *"personnel"* includes employees/staff/officials supplied by labour brokers or service-providers to the Municipality.

This policy refers to "users" as all computer users at the **MDM**, whether they are permanent, on contract or temporary employees.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose personnel use Municipality's computers or IT infrastructure.

2.5 POLICY STATEMENT

2.5.1 COMPUTER SYSTEMS AND EQUIPMENT OWNERSHIP

All computer equipment, printers, software licenses, network and data that employees use at the Municipality shall at all times remain the property of **MDM**.

If an employee has been issued with computer equipment by the ITO on behalf of **MDM**, by signing a declaration form such an employee accepts full responsibility for the safekeeping and proper use of the said equipment and accessories while in his/her possession.

2.5.2 ACQUISITION AND ALLOCATION OF COMPUTER EQUIPMENT

At the request of the employee's manager, accompanied by a signed appropriate Application for IT Equipment Form, computer equipment may be procured through **MDM** Supply Chain Management and an employee may have access to computer-based services. These are provided to assist the employee to fulfil his/her official duties and/or business activities. The ITO shall set the qualifying criteria and it shall be documented and approved by the Municipal Manager.

New equipment will be procured only if current equipment does not comply with the minimum standards set for the computer equipment. Printers are allocated in the same way but employees will be expected to share printers with other personnel.

In cases where an employee requires the allocation of non-standard equipment or software to fulfil their duties effectively, the employee's senior manager or head of the section must make a recommendation in the form of a motivated submission to the ITO. The submission must include the details and where possible the cost of the software or equipment required.

2.5.3 MANAGEMENT OF IT EQUIPMENT

The ITO is responsible for the management of IT Assets in accordance with **MDM** Asset Management Policy and the Asset Life Cycle Management Processes including standards, acquisition management and long term planning. Authority to acquire IT assets (and any other assets) is as set out in the Supply Chain Management Policy of **MDM**.

2.5.4 STANDARDS

2.5.4.1 Standard issue personal computer

To make for cost-effective use of equipment and software, the Municipality will standardize on core set of software and hardware product requirements. The specifications will be set and revised from time to time by the ITO. The standards will cover the following:

- Minimum specifications for current desktop computers. Users may only request new computers if their current computers do not comply with the minimum specifications set by the ITO. (Annexure A);
- Hardware specifications for standard issue desktop computers, notebook computers and printers. Users will be issued with a computer that meets this standard. When the standard is raised, computers below the standard can be upgraded or replaced, if the computer is found to be inadequate by the ITO, it will be upgraded or replaced;
- Specifications for new desktop computers, notebook computers or printers;

- When the Municipality buys a new computer or printer, its specification will conform to this standard. The ITO will normally follow the standard set by the State Tender Board or SITA's Information Technology Acquisition centre;
- Standard issue software set. A list of software that will be installed on all computers by default;
- Additional software set. A list of software that may be installed if needed to do the job. To control maintenance cost, no other software may be used without the written approval of both the user's Manager and the ITO.

2.5.4.2 Non-standard items will not be supported

The ITO supports a large number of products - both hardware and software. To keep costs down IT Support limits the product range it will support and provide training for. If an employee uses software that falls outside this product range, the ITO cannot guarantee support for such a product. All reasonable requests will be considered and where the majority of employees require a non-standard product, the ITO will consider adding it to the list of supported items.

2.5.5 ALLOCATION OF PERSONAL COMPUTERS AND LAPTOP COMPUTER TO EMPLOYEES

Employees are not entitled to both laptop computer as well as desktop personal computer (unless authorized by the head of the Directorate, i.e. the Director and the ITO) for a specific reason. An employee may not request that laptop computer be procured, if such an employee is already in possession of desktop computer and vice versa. If an employee is in the possession of a desktop computer and requires a laptop computer, the desktop computer will be cascaded to next line personnel or be kept in the ITO storeroom or returned to **MDM** Asset Management Unit. Exceptions will only be made under exceptional circumstances on motivation by submission of a memorandum to the head of the Directorate for approval, after motivation from ITO, attached to the standard **Application for IT Equipment Form**.

Submissions for the requirement of mobile/laptop computers/equipment issued on pool-type basis will be considered by the ITO on approval, after recommendation by ITO, of a memorandum submitted to the head of the Directorate attached to the standard Application for IT Equipment Form.

2.5.6 USAGE OF IT EQUIPMENT

2.5.6.1 Classification of Computer Users

Employees are classified into two categories according the nature of their work. **Standard users** are employees who only use standard applications installed on their personal computers. **High-level users** are employees who use standard software and additional applications used in their divisions e.g. Financial Systems or GIS.

2.5.6.2 Use of computer equipment for official purposes

Computer equipment is issued to employees for official duties and for Municipality's business or activities sponsored or authorized by the Municipality.

2.5.6.3 Use of computer equipment for non-official purposes

Occasional and brief use of computer equipment by employees for personal use is allowed, but not encouraged, subject to the following restrictions:

- Personal use should not hinder productivity;
- Only incidental amounts of employee time, time periods comparable to reasonable breaks during the day, should be used to attend to personal matters;

- Personal use should not cause the Municipality to incur a direct cost in addition to the general overhead.;
- Employees may not install or use software that does not support official business or activities sponsored by the Municipality, for example games, screensavers, screen utilities, movies, songs not on original CD, pictures, etc.;
- Personal use shall comply with all other terms of this policy;

2.5.6.4 Storing of material on computer equipment

Users should take care not to expose the Municipality and its employees to materials or information that could be considered offensive. This includes words, images of any kind and/or recorded sounds (audio). If an employee becomes aware of offensive material stored by another employee on **MDM** computers, networks and servers, such employee has a duty to report the offensive material stored the employee to the ITO.

Storing of the following material is expressly prohibited:

- Discriminatory, intolerant or derogatory material based on race, religion, gender, age, ethnic or social origin, sexual orientation, disability, physical condition, HIV status, conscience, belief, political opinion, culture, language or birth;
- Any form of violence, pornography, explicit nudity, sexual acts, gross depictions, religious content deemed inappropriate by other religious groups, militant or extremist material

2.5.6.5 Computer Equipment should be switched off after hours

Unless computer equipment has to run after working hours to complete an official task, all employees should log off the network and switch off their equipment at the end of each working day. Not logging off the network when computer is not being used or after working hours shall constitute breach of Municipality's IT Security Policy. Switching off of computer equipment is considered best practice to reduce the risk of fire, save energy and ensure that any documents that employees have worked on are properly closed and ready for backup.

2.5.6.6 Computer Equipment should be logged into the network

The Municipality provides its computer users with access to networked services and resources. The Municipality is also running Microsoft Windows Domain, and maintains security of the network through it. Computer maintenance and support is also done remotely via the network. Computers that are not logged onto the network cannot access networked services and resources, and cannot be maintained remotely. Computers that are not logged onto the domain poses a security risk to the Municipality's computer network. For these reasons, employees may not use computer equipment without first logging into the Municipality network when in the municipality premises where network has been provided. Employees must remain logged in when using computers. A support account will be created automatically on each workstation for support purposes.

Employees must lock their workstations when they are not working on their computers or are out of the office. It is advisable that the workstation must have password protected screensaver that will be activated automatically after few minutes (typically ten minutes) of inactivity on the workstation.

2.5.6.7 Work should be saved on the network storage allocated

Employees are advised to save all computer-based work they produce on the home folder (**H:** network drive), which is central data repository allocated to each user on the files servers of the Municipality. This home folder (**H:** network drive) will be made available offline to allow users to access their saved working files while not connected to the network and synchronise all changes or addition when connecting back to the network. This home folder will be made the default location of the 'My Documents' folder for all users. By default, all users will save their working files (e.g. Excel SpreadSheet, Word documents, PowerPoint Presentations, etc.) on their home folder, unless explicitly excluding files. All multimedia files like music, pictures, and video should not be stored on the home folder, unless they are work related.

The Municipality provides employees with network-based storage. Each user has home folder (**H:** network drive) on the network. This holder will have storage space restriction determined by the ITO with view of optimizing file server storage (unless otherwise authorized by the ITO). If failure does occur, or users lose their workstations (computers and laptops connected to the network), working files stored on the network storage can usually be recovered from back up. If employees are producing work that needs to be shared, the employees should request the ITO to create a shared folder on the network. Such requests will be submitted on a memorandum to the ITO stating reasons for such a request.

Employees may not save files on any of the network drives that are unrelated to Municipality business. Any private or personal files should be saved by employees on removable media and not on the local drive of their computers. ITO will not take responsibility for data or working files saved on the local drive of workstations or the removable storage unless permission to do so has been explicitly been granted by ITO.

2.5.7 INSTALLATION OF HARDWARE AND SOFTWARE

2.5.7.1 Only authorized support staff may install or copy software

To avoid breaking the law, the Municipality has to carefully control the software licenses it owns. For this reason:

- Only authorized IT Support staff may install or upgrade software on a Municipality computer. A valid license must be allocated to each installation;
- Only authorized IT Support staff may copy computer programs. A program may be copied for official purposes only if allowed by the EULA. A user may be held personally liable for any damages, and legal costs, if he or she copies software illegally;
- Maintaining central control over licenses and installations also protects the users from unknowingly breaking the law.

2.5.7.2 Personal software may be provided, within limits

There are circumstances under which users may be allowed to provide their own software, or software licensed to a service provider or duly authorised third parties. In this case, the employee must provide documentary proof that the employee holds a valid license before the software will be installed. The Municipality has the right to hold the license until the software is removed. The Municipality will not replace a license if it is lost, nor offer compensation. Only authorized IT Support staff may install the user-provided software.

2.5.7.3 Software Written by MDM

The **MDM** will normally own the copyright for software written "in-house", by the Municipality. Such software may be used within the Municipality without a license. However, such software programs still have to be installed by authorized IT Support staff. The personal use of such software will be as determined by **MDM** from time to time as the need arise, and users will require explicit authorization by the Municipality. Since the copyright of in-house developed software will be owned by **MDM**, all copyright laws are applicable and unauthorised copy, use and/or distribution of such in-house developed software is an offence.

2.5.7.4 Use and Storage of Unlicensed Software

Unlicensed software is illegal and not allowed on any computer owned by the Municipality. The Copyright Act 98 of 1978 protects intellectual property against theft. If an employee uses software without a license, the employee may be found guilty of a criminal offence. The author of the software may also seek civil damages. If an employee knows or suspects that software on computer equipment is unlicensed, the employee must contact the ITO. If employees infringe on applicable licensing and copyright laws the Municipality will hold such employees liable for criminal or civil action.

2.5.7.5 Responsibility for offensive material

MDM is not responsible for offensive material stored on Municipality computers, networks and/or servers in violation of MDM policies if viewed by an employee, either by accident or intention. All employees use their computer at their own risk. If an employee becomes aware of any offensive material on his/her computer or those of other users, or on MDM network or servers, they should report such to the ITO.

2.5.7.6 Managers may monitor software used by staff

The Municipality has right, but not duty, to monitor any aspect of its computer system, including use of the software on its computers. Monitoring is justified by the need to apply this policy and to measure software usage for licensing purposes and/or effectiveness of software. Managers may monitor particular software program, used by individual staff members or used by group of staff member or general staff.

2.5.8 USE OF MDM RESOURCES

Employees shall take care to use all computer equipment and resources in a responsible, ethical and lawful manner. No employee should waste computer resources or unfairly prevent others from the use of such resources.

Employees may **not** use the Municipality's computer facilities to:

- Play games or run other entertainment software, unless the ITO has provided this software as standard software;
- Save files containing images, music, sound or video onto Municipality servers, unless they are for official purposes. In such official cases an employee computer's local hard disk shall be used to save such material. This is usually the C: drive. Authorization to do so should be obtained from the ITO;
- Make or store illegal copies of material protected by copyright. This includes software programs and publications, in whole or in part;
- Back up their local hard drives onto Municipality servers.
- Print large documents if there is viable on-screen alternative.

2.5.9 MAINTENANCE AND MANAGEMENT OF COMPUTER EQUIPMENT

2.5.9.1 Employees have duty of looking after equipment issued to them

Employees are expected to take good care of Municipality computer equipment issued to them. This is particularly relevant to staff who use portable equipment such as notebook computers, mobile 3G modems and flash disks. Employees must take reasonable precautions against loss and damage. Loss, Theft, and damage of computer equipment allocated to employees shall be dealt with in line with the applicable Municipality policies and laws applicable in the Municipality such as Municipal Finances Management Act, Asset Management Policy and Procedures, SALGBC Collective Agreements, and/or Fraud Prevention Policy.

2.5.9.2 Lending of Computer Equipment

Employees who borrow or lend equipment (pool laptops or mobile printers) from IT for usage should fill in the ITARF and specify when they will return the equipment. It is the responsibility of the employee to make sure the equipment is kept safely and returned to IT in good working order. In cases where theft, loss, or damage of such equipment lent to users occurs, it shall be dealt with in accordance with the applicable municipality laws and policies.

2.5.9.3 Employees must obtain Equipment removal control form before taking equipment off-site

Employees may need to take equipment (printers and/or pool laptops) off Municipality premises, either to work at home or at another satellite office. Employees must obtain equipment removal control forms from the ITO. (If equipment needs to be removed outside of normal working hours the employee's manager may authorize such removal. The ITO must be notified if this occurs). The form must indicate the employees' name as well as the description and serial numbers of equipment to be removed. The form must also indicate an expiry or return date. Permission is implicitly granted to employees to take pool laptops home provided the Equipment Removal Control Form has been completed and duly signed.

2.5.9.4 Employees may not install, move, and tamper with computer equipment

Only authorized IT Support personnel may move, upgrade or repair computer equipment. Employees may not remove, install or tamper with any internal component of computers or the peripheral equipment that may be attached to it (e.g. printer). Employees may not move computer equipment to another room, or site - unless it is specifically designed to be carried around (e.g. laptop computers). Employees may not swap equipment with other users. Moving or swapping equipment will create inconsistencies in the asset register. Employees should contact the ITO, who will arrange for the equipment to be moved or installed for them.

Employees have to complete **ITARF** forms for any computer equipment that is removed from their control. This includes equipment removed for upgrade or repair.

Users may open printer to remove or replace paper as well as toner or print cartridge.

2.5.9.5 Upgrade of Computer Equipment

New equipment will be provided only if current equipment does not comply with the minimum standards set for the computer equipment. The replace will be done in the following manner:

- The end user initiates the process of approval and procurement of new equipment, replacing the outdated equipment as described in Acquisition, Delivery and Installation Process of Life Cycle Management – Stage 1.

- The end user completes an **ITARF** by which the responsibility/accountability for the old equipment is transferred to IT for safekeeping and/or testing and write offs. This will then follow the Termination Process of Life Cycle Management – Stage 3.
- The end user hands the original **ITARF** to the ITO while he retains copy. An ITARF must be completed and signed by the user and the ITO to transfer the equipment to IT for testing. A copy will be kept by the user.
- The IT Technician will change the status of the equipment "To be Tested" on the IT asset register.

2.5.9.6 Lost or Stolen Equipment

If an employee loses or damages equipment, software or data that belongs to the **MDM**, the employee must promptly report **in writing** to the Head of the Directorate, Asset Manager in the Budget & Treasury Office and the ITO. In the case of theft or suspected theft, the employee must also report the loss to the South African Police Service within 24 hours of the loss being discovered.

- In terms of the Municipality practices and policies, the user must provide the ITO with the following information:
    - Serial number of the IT Asset that was stolen or lost.
    - Case reference number of the South African Police Service (SAPS).
    - Date it was stolen and short description of what happened.
- The ITO will then change the Status of the item(s) to "Stolen/Damaged".

However, the above procedures do not replace the procedures outlined in the Municipality's Asset Management Policy and other applicable laws and policies. The responsibility of reporting the loss, theft, or damage of the Municipality computers to the duly appointed Asset Manager or as prescribed in the Municipality policies or any applicable laws and directives remains with the employee under whose care and allocation the loss, theft or damage occurred as per **MDM** asset register. At all times, the prescripts and procedures of the **MDM** Asset Management Policy, Municipal Finances Management Act, and all other applicable laws and policies dealing with such, shall supersede this policy in cases where contradictions/conflicts/inconsistencies arise.

2.5.9.7 Damage of Computer Equipment

- Computer equipment that has been damaged wilfully or as consequence of negligence must be transferred between a user and an ITO by means of an **ITARF**.
- The end user will complete the **ITARF** and supply the ITO with copy, which will provide detailed report that will also serve as information to support decision to be taken on the liability for the repair costs of damaged equipment.
- After the repair costs and the circumstances have been established the end user will be notified of the outcome. As in the case of stolen assets the ITO must be notified and all other procedures set out in other policies such as **MDM** Asset Management Policy.
- The ITO will update the IT Asset Register of the outcome of the decision to replace or to repair the damaged equipment.

2.5.9.8 Employees may have to pay for lost, damaged or stolen equipment

If an item is lost, damaged or stolen while it was under an employee's control and/or responsibility, **MDM** will not normally ask the employee to pay for it. But, employees may lose this cover if they fail to follow treasury regulations or standing instructions as prescribed in **MDM** Asset Management Policy, and all other applicable laws and policies. The main elements are summarized here, but this summary does not replace the original prescripts which will be used to deal with any loss.

An employee may lose liability cover against loss if the employee:

- was not conducting official business when the loss occurred;

- was under the influence of alcohol or drugs when the loss occurred;
- had not been issued with a permit to take the item off Municipality premises;
- did not obtain a receipt for equipment voluntarily surrendered by an employee;
- acted recklessly or negligently;
- intentionally caused the damage;
- ignored any standing instructions i.e. Finance procedures;

2.5.9.9 Movement or Change of Location of Computer Equipment within MDM

End users, who intend to move computer equipment will complete the standard **ITARF**, keep a copy and forward the original to the ITO before the equipment can be moved. The ITO will do physical verification between the **ITARF**, the equipment and the IT asset register, before as well as after the move of location. The IT asset register will be amended with the end user's new physical location and contact details.

2.5.9.10 Computer equipment of Officials who resign

- When an official resigns he/she must return IT Assets in good working condition.
- It is expected from all end users to sign off their responsibilities with regard to all the computer equipment that has been issued and entrusted to them when they leave by means of the Municipality Employee Exit Checklist that s/he obtains from the Human Resource Unit of **MDM**.
- The ITO will check if the content on the form completed by the user corresponds with the IT asset register and the physical IT assets.
- The user must also complete the ITARF and provide it to the ITO for the Asset register database to be updated.

2.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this Policy. The Policy will be applied in several ways:

- Where technology allows, the policy will be enforced automatically. Management reports will highlight possible violations. These will be investigated to identify actual violations. The offender's manager will take disciplinary action in line with Municipality policy.

- Users may self-police the policy by reporting any violations via the grievance procedure.

- The ITO may issue specific instruction.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the Collective Agreement on Conditions of Services. Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

2.7 COMMENCEMENT AND REVISIONS OF POLICY

This policy takes effect from the date determined by council in the resolution for its adoption or as soon as signed off by the Municipal Manager, and will be reviewed annually or as the need arises, whichever comes first. The policy may be amended from time to time as the need arises. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on the Municipality Website or Intranet, or by way of e-mail or memorandum.

3. USER ACCOUNT AND PASSWORD MANAGEMENT POLICY

3.1 INTRODUCTION

Access to sensitive Mopani District Municipality (**MDM**) information by unauthorised persons could result in legal liability, substantial financial losses, violation of personal privacy and embarrassment to the Municipality. The Municipality computer networks, which connect to the outside world through the Internet, are no longer isolated from the potential of unauthorised access. With the use of computers and computer networks in the Municipality, and with the Municipality computers connected to the World Wide Web, it is important that **MDM** implements controls to protect access to Municipality information, data, computers and computer networks from unauthorised.

It is an accepted principle that MDM can never conduct its business of service delivery without deploying the use of Information Technology, computers, and computer networks. However, this principle must be tempered by the fact that access to Municipality information carries with it the responsibility to protect privacy, confidentiality and integrity. Unauthorised access to the Municipality's information or systems has been identified as a major information security risk that must be proactively managed.

Access to Municipality IT resources by unauthorised people or computer processes can result in:

- the Municipality's sensitive information being compromised;
- non-compliance to legal and regulatory requirements;
- prosecution through non-adherence to legislation;
- adverse impact on the Municipality's image and reputation;
- litigations due to inaccurate decisions based on data without integrity and information leaked to third parties;

3.2 BACKGROUND

Formal procedures must be in place to control the allocation of access rights to computers, computer networks, Information Technology systems and services. The procedures must cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to computers, computer networks, and information systems and services. Special attention must be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

3.3 PURPOSE OF THE POLICY

The purpose this policy is:

- To establish direction, procedures and requirements to ensure the appropriate management of User Accounts for access to computers, computer networks, data and information handled by the Municipality computer resources;
- Establish minimum rules, guidelines and standards for passwords creation and management used to logon to Mopani District Municipality computers, computer networks, and information systems;
- Define standard user access roles for common job categories;

3.4 SCOPE OF THE POLICY

The scope of the policy covers those people who make use of MDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "USERS". Users are all permanent, contract and temporary personnel employed by the **MDM** who have been issued with a Municipality's Computer.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the Municipality's computers.

3.5 POLICY STATEMENT

3.5.1 Directorates Requirements For System Access

Access to computer networks and information systems and resources, and associated data will be controlled on the basis of requirements of various directorates. Access and allocation of these I.T resources will be carried out in terms of **MDM** IT Asset Management Policy, and following procedures defined in that policy. All users are required to abide by all policies related to use of Information Technology in **MDM**.

3.5.2 Access controls

- Access controls will be established for all major information, information systems and facilities based on their classification and security risk assessment to ensure that the appropriate level of security is implemented;
- Logical access controls will be implemented in accordance with this policy and the Information Security Policy. Physical access controls will be implemented in line with this policy and the Physical and Environmental Security Policy;
- Access to the network, information systems and servers will be achieved by the use individual user accounts (UIDS) that will require an appropriate authentication method as outlined in the Password and Authentication Policy;
- Access to information systems and facilities will be governed by a formally defined authorization process covering the creation, modification/maintenance, re-enabling and deletion of accounts;
- Users will only be granted access to information and information systems and facilities on a "need-to-know" basis. Users will only be granted the minimum access and privileges required to perform their duties;
- Procedures will be implemented to ensure that access to data or information is not dependent on any one individual. Privileges granted by groups will be implemented in order to facilitate this function;
- Each assigned account will uniquely identify the user and must conform to the Municipality's naming standard (making use of the users name and first initial) or an appropriate coding structure. Accounts must not give any indication of the user's access rights;
- Security of systems administration accounts and passwords will be the responsibility of the technical owner of that system and must adhere to the Council policies with the exception of where this is not technically possible;
- A notice warning users about accessing information without authorisation will be displayed before users can gain access to any information system or facility. It should not identify any information about the information system or any other internal matters;

- A review period, determined by the information "owner", will be established to reassess the access controls implemented for information, information systems and facilities. A record of the review must be maintained;
- User accounts will be reviewed on a regular basis to ensure access and account privileges remain applicable to the job function/role or employment status of the user. A record of the review must be maintained;
- All employees have a legal duty to keep all personal data confidential and to comply with the data protection provisions contained within the Code of Conduct for Employees;
- Access to information systems and facilities will be revoked for users who do not need access to perform their duties in order to ensure the confidentiality, integrity and availability of information to other users.

3.5.3 Account Management

- Accounts will only be created and maintained for users that need access to information, systems and facilities to perform their official duties on behalf of the Municipality;
- User accounts will only be authorised to the capabilities appropriate to the user's role requirements, responsibilities or specific needs to carry out a function for which they are employed. Users will only be assigned the access privileges needed to carry out their job function;
- All accounts created or modified must have a documented request and the appropriate authorisation. A record must be maintained of all authorisations including the access rights and privileges granted;
- Procedures will be established to ensure user's access rights and privileges are adjusted in a timely manner whenever there is a change in a user's status;
- User accounts will not be activated until the authorisation process has been correctly completed. Users must not have access to information systems until all activities relating to the commencement or resumption of employment have been completed i.e. acknowledgement of Acceptable Use Policy;
- Generic or shared accounts will not be permitted. The only exception will apply to email accounts required by services were Information & Data Management Section has granted approval;
- Upon notification of termination, transfer, resignation, suspension or retirement from employment received from the relevant authoritative source(s) the user account will be disabled/de-activated. Disabled accounts will be deleted after the period specified in the Access Control Standard;
- Each user account must be unique, only connected with the user to whom it was originally assigned. *Reuse of user IDs is not permitted*;
- All user accounts will as a minimum force the use of a password;
- All default passwords for accounts must be constructed in accordance with the Municipality's Password & Authentication Policy. All default passwords must be immediately changed by the user immediately after logging into the system if not prompted automatically to do so;
- User accounts with system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by the user.

3.5.4 Password Management

The allocation of passwords should be controlled through a formal management process (documented in the Password Policy) and this process should include the following requirements as a minimum:

- Users should be required to sign an undertaking to keep personal passwords confidential. This signed statement could also be included in the terms and conditions of employment.
- If users are required to maintain their own passwords, they should be provided with a secure initial password, which they should be required to change immediately at first logon.
- Procedures should be established to verify the identity of a user prior to providing the user with a new, replacement or temporary password.
- A secure procedure should be followed when granting users temporary passwords and the use of unprotected (clear text) electronic mail messages should be avoided.
- Temporary passwords should be unique and should conform to password standards.
- Users should acknowledge receipt of passwords.
- Passwords should never be stored on computer systems in an unprotected form.
- Default vendor passwords should be replaced as soon as the installation of systems or software has been completed.

3.5.5 Privilege Management

The allocation and use of privileges should be restricted and controlled. Inadequate control of system administration privileges can be a major contributing factor in failures or breaches of systems. A formal authorisation process should be used to control the allocation of privileges in multi-user systems that require protection against unauthorised access. The following steps should be considered:

- The access privileges associated with each system product, e.g. operating system, database management system and each application, as well as the users to which they need to be allocated, should be identified.
- Privileges should be allocated to users on a need to-use basis and on an event-by-event basis, i.e. the minimum required for their functional role and only when needed.
- An authorisation process and a record of all privileges allocated should be maintained.
- Privileges should not be granted until the authorisation process is complete.
- Privileges should be assigned to a different user ID than that used for normal business activities.
- Changes to privileged accounts should be logged for periodic review.

3.5.6 Logging and Monitoring of Access/User Activities (Events)

Auditing will be implemented on all information systems to track access and record events in line with the good industry practice and for purposes of enforcing this policy and all other I.T related policy.

A set of controls should be defined for controlling and monitoring user access to and activities on systems. The following should, inter alia, be considered:

- Repeated failed login attempts should be identified and investigated.
- Any blocked or suspended user ID (three or more consecutives failed attempts) should be investigated to verify that the user is the authorised owner of the user ID and not an unauthorised person trying to discover passwords.
- Inactive users should be monitored and corrective action should be taken after a predefined period of inactivity, e.g. users that have been inactive for 60 days should be blocked.
- Activity carried out by default users (e.g. guest, administrator, owner and root) should be monitored on a daily basis.
- Access to critical accounts, log files, data files and databases should be monitored.

- Periodically, logs should be reviewed to monitor the activities of privileged users and failed access attempts.
- The organisation should be prepared to react appropriately should a breach of access such as an unauthorised intrusion be detected.
- Periodically, the organisation should check for and remove or block redundant user IDs and accounts.
- The activities of the privileged or super user login account should be closely monitored and reviewed by senior computer security management.
- Users' passwords should be reviewed to ensure that an appropriate level of complexity is maintained.

3.5.7 Unattended Users Equipment

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities in regard to the implementation of such protection. Users should be advised to, inter alia:

- terminate active sessions when finished, unless such sessions can be secured by an appropriate locking mechanism, e.g. a password-protected screen saver;
- log computers off at the end of a session (i.e. it is not sufficient to merely switch off the PC screen or terminal);
- when not in use, secure computers from unauthorised use by means of a key lock or an equivalent control, e.g. password access;

3.5.8 Exceptions

- Exceptions to this policy will only be granted if:

  (a) Compliance would adversely affect the ability of the service to accomplish a mission critical function; or
  (b) Compliance would have an adverse impact on the service provided or supported by the information, system or resource; or
  (c) Compliance be achieved due the incapability of the information system or a resource

- A procedure for requests for exception to this policy will be produced and implemented

3.5.9 Responsibilities

3.5.9.1 Human resources division is responsible for:

- Providing all employees with copies all I.T policies that govern the use of information technology resources and ensuring that the Information Technology Acceptable Use Policy is acknowledged by signed signing Information Technology Acceptable Use Acknowledgement form;
- Proving ITO with copies of all User Account Termination forms.

3.5.9.2 Line managers/supervisors are responsible for:

- Promptly notifying HR when permanent and temporary employees, contractors and service partner personnel terminate employment or transfer to new duties or responsibilities;
- Promptly notifying the relevant systems administrators when staff, contractors and service partner personnel terminate employment or transfer to new duties or responsibilities;
- Providing all temporary employees employed within their directorate/division with a copy of the Acceptable Use Policy ensuring it is acknowledged/signed for by the individual.

3.5.9.3 All Users are responsible for:

- Familiarizing themselves with this policy and all other related policies and guidelines set out below;
- All activity related to accounts they have been allocated;
- Reporting any suspected misuse of accounts/passwords to their line manager or the ITO;
- Ensuring the security of their own passwords and reporting any potential compromise to the security of their user accounts to their line managers or the ITO.

3.5.9.4 Information Technology Office is responsible for:

- Maintaining this policy;
- Ensuring processes associated with the above are documented in formal procedures.

3.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "Electronic Mail Policy". These duties include, but are not limited to:

- Investigation of alleged or suspected non-compliance with the provisions of this policy; and
- Suspension of service to users, with or without notice, when deemed necessary for the operation and/or integrity of the Municipality's communications infrastructure, connected networks, or data.
- The ITO is able and reserves the right to monitor and/or log all network activity without notice, including all e-mail and Internet communications. Therefore, users should have no reasonable expectation of privacy in the use of these resources.
- While the **MDM** will not regularly monitor electronic- mail, users are on notice that the maintenance and operations of electronic message systems may result in observation of random messages. E-mail messages are not personal and private. E-mail system administrators will not routinely monitor individual staff member's e-mail and will take reasonable precautions to protect the privacy of e-mail.
- However, management and ITO staff may access a user's e-mail:
  - ✓ For a legitimate business purpose (e.g. the need to access information when a user is absent for an extended period of time).
  - ✓ To diagnose and resolve technical problems involving system hardware, software or communications; and/or to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

- ✓ By participating in the use of networks and systems provided by the **MDM**, users agree to be subject to and abide by policies governing their usage. **MDM** management will review alleged violations of this policy on a case-by-case basis.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the Memorandum of understanding on Conduct of Service 0f 1994.

Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

3.7 COMMENCEMENT AND REVISION

This policy takes effect from the date of its adoption by a council sitting or as shall be determined by council as shall be indicated in the council resolution and will be reviewed annually. The policy may be amended from time to time. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on municipality Intranet or website and/or by way of e-mail.

4. IT SECURITY POLICY

4.1 INTRODUCTION

Increasingly, municipalities 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 Mopani District Municipality offices. This document shall be read in concurrence with the Minimum Information Security Standards (MISS).

4.2 BACKGROUND

Management of Mopani District Municipality must set a clear policy direction; demonstrate support for, and commitment to, information security through the issuing and maintenance of a consistent information security policy throughout the organisation, including the enforcement thereof through appropriate disciplinary procedures and actions.

4.3 PURPOSE OF THE POLICY

The purpose of this policy is to provide the Mopani District 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 Mopani District Municipality information.

4.4 SCOPE OF THE POLICY

The scope of the policy covers those people who make use of MDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "USERS". Users are all permanent, contract and temporary personnel employed by the **MDM** who have been issued with a Municipality's Computer.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the Municipality's computers.

4.5 POLICY STATEMENT

4.5.1 INFORMATION SYSTEMS SECURITY

4.5.1.1 Individual Accountability

- All personnel who use/access/perform any function on or manages any part of the Mopani District Municipality Information Technology Systems are responsible and accountable for following appropriate recommended procedures and for taking all possible steps to safeguard the information handled by that system and any sensitive assets involved.

All Information Technology Systems shall provide means by which individual users can be uniquely identified and held individually accountable for their actions, in respect of which the system shall provide for appropriate records.

- All users of the Mopani District Municipality Information Technology systems are responsible, within the span of their control, to ensure that no actions are taken which could degrade or compromise the confidentiality, the level of accuracy, completeness, dependability and responsiveness levels of the programmes, services and information handled by the system.

- Users of the systems shall report any observed or suspected action/security weaknesses in, or threat to, systems or services to IT SECTION.

- ITO is the overall custodian of security of Information Technology Systems.

4.5.1.2 Controlled Access

- An employee of the Mopani District Municipality shall be granted access to only the classified level of information and assets for which appropriate access authorization(s) and the need to know have been approved.

- A person shall be granted access to only those Information Technology system resources necessary to perform the assigned functions and only when such access will not lead to a breach of this or any other security principles.

- Appropriate segregation of duties, specifically allocated and defined in writing, shall apply.

- Controlled access will be achieved via physical and procedural means. Unique identification of the user to the system must be provided. An access authorization structure shall determine access and privileges, grant such access and privileges and record, control and monitor these.

4.5.1.3 Levels Of Protection

- The protection applied to information technology systems shall be commensurate with the sensitivity levels of the information and assets involved and shall take into consideration the identified threats to and vulnerabilities of the information system.

- Risks or threats that Information Technology systems are exposed to shall be identified, analysed, evaluated and quantified in terms of the probability of them occurring and the potential impact of such an event of the Mopani District Municipality and its activities. A documented security plan should exist to manage risk situations, which should be revised on a regular basis.

4.5.1.4 Disaster Recovery Plan

An approved disaster recovery plan and procedures should exist to minimize the impact of any type of disaster on the Information Technology Systems. It should be classified as Top Secret and handled on a need-to-know basis.

4.5.1.5 Security Education

Officials who have access to systems should be subjected to a programme of effective and appropriate security education to foster their security awareness on risks and the approved Information Technology system principles.

4.5.1.6 System Access Control and Password Security

- Access to computer systems shall be controlled by means of an approved computer access control system which identifies the authorized user and verifies his/her identity.
- The access control system shall update an audit trail of all authorised and unauthorised efforts to gain access to the computer systems. Unauthorised access attempts shall be considered a breach of security.
- Passwords shall be individual and exclusive, and shall not be disclosed without authorisation in forced exceptional cases, and without documenting the incident. Unauthorised disclosure of passwords shall be considered a breach of security.

4.5.1.7 Desktop and Laptop Security

- Desktops shall be located in a physically protected environment where access control measures have been instituted and are applied consistently. Unattended equipment shall have appropriate security protection.
- All computers, both desktop and laptop (notebook, netbook, and tablet) computers are to be managed as outlined in the MDM IT Asset Management Policy.
- Access to computers on which classified data is processed, shall be controlled and limited by means of approved access control software.

4.5.1.8 Physical Security

Areas where computer-related equipment are accommodated, or office areas where classified information is dealt with, shall be protected in such a way that unauthorised access is prevented. Access control systems and procedures should regulate, record, and monitor movement of all persons in these areas.

4.5.1.9 Utilization of Private Computers

When private computers are to be used, written approval shall be obtained from ITO for use of privately owned computers 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.

4.5.2 INFORMATION TECHNOLOGY COMMUNICATION SECURITY

Communication of information of classified nature to could be communicated, electronically or verbally, is to transmitted in a safe and secure environment.

4.5.2.1 Security of Data Transmission

Communication pertaining to classified information should be encrypted in line with the Mopani District Municipality approved cryptographic devices.

4.5.2.2 Modem/Dial-Up Connections

No modems shall be connected to communication networks without the authorization from ITO. Authorisation shall only be given on receipt of a detailed motivation approved by the Senior Manager of the particular employee 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.

4.5.2.3 Electronic Mail

The use of electronic mail and internet is governed by the MDM Electronic Mail and Internet Acceptable Use Policies.

4.5.3 IT SECURITY SYSTEMS CONTROLS

4.5.3.1 IT Security and Computer Viruses

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

- If any desktop, laptop, or server computer poses a risk to the computer network, other hosts or service delivery, the culprit desktop, laptop, or server shall be disconnected from the network until the risk has been resolved.
- Access to any desktop or laptop or server shall not be prevented by any logical or physical means. Default access granted by the network may not be removed.
- All desktops, laptops and servers shall use the latest security patch levels, as approved and distributed by ITO.
- The computer name of all desktops, laptops and servers shall contain the exact username of the owner, unless authorised by ITO.
- ITO shall maintain antivirus software to protect the municipality network against any virus attacks.

4.5.3.2 Firewall and Perimeter Security

The municipality computer network is to be protected from the internet and non-secure networks with firewalls and Intrusion Detection and Prevention systems.

- External network connections to the internal network may only be used for the purpose(s) it was authorized and intended for. All services being accessed from external or non-secure networks shall use secure protocols.
- Wireless devices and VPN access are not allowed on the Mopani District Municipality network, unless provided by ITO.
- Remote Access Services dial-back shall be activated and only to a pre-defined and authorized telephone number.
- ITO has to approve all exceptions to abovementioned connection requirements.

- Virtual Private Network extensions are only permitted making use of secure tokens, managed and supplied by ITO.

4.5.4 SECURITY BREACHES

All employees have the responsibility to report any incident of security breach to the ITO.

Breaches of security shall at all times be dealt with using the highest degree of confidentiality in order to protect the official(s) concerned and prevent him/her from unnecessary injustice and the integrity of MDM.

4.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "IT Security Policy". These duties include, but are not limited to Investigation of alleged or suspected non-compliance with the provisions of this policy.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the applicable policies of MDM and applicable laws of RSA.

4.7 COMMENCEMENT AND REVISION

This policy takes effect from the date of its adoption by a council sitting or as shall be determined by council as shall be indicated in the council resolution and will be reviewed annually. The policy may be amended from time to time. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on municipality Intranet or website and/or by way of e-mail.

5. INTERNET ACCEPTABLE USE POLICY

5.1 INTRODUCTION

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 un-trusted networks and to ensure that internet resources are utilized in a manner which does not adversely impact normal business operations.

5.2 BACKGROUND

Mopani District Municipality (**MDM**) provides internet and World Wide Web access to all its employees and employees are cautioned that many of the web pages on the World Wide Web 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 **MDM** implements and deploys adequate measures to govern and regulate 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 **MDM** is governed by this Internet Acceptable Use Policy.

5.3 PURPOSE OF THE POLICY

The purpose of this policy is:

- To define security "laws and governance" that shall be enforced Municipality wide to ensure that **MDM** internet information systems are adequately protected from misuse or direct/indirect exposure to security risks;
- To ensure the highest possible level of Confidentiality, Availability, Reliability and Integrity for the MDM network, Information and information systems;
- To encourage cost-effective and productive use of MDM internet systems;
- To clearly define user responsibilities and liability when using Municipality internet facilities in day-to-day activities;

- To ensure compliance with regulations of Republic of South Africa (RSA) and other relevant international laws, regulations, standards and best practices.

5.4 SCOPE OF THE POLICY

The scope of the policy covers those people who make use of MDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "USERS". Users are all permanent, contract and temporary personnel employed by the **MDM** who have been issued with a Municipality's Computer.

This policy refers to "Users" as all computer users at the **MDM**, whether they are permanent, on contract or temporary employees supplied by service-providers to the Municipality.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the Municipality's computers.

5.5 POLICY STATEMENT

Internet users are expected to use internet facilities of **MDM** 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 **MDM**. Access to internet facilities of **MDM** is a privilege that may be wholly or partially restricted by the Municipality 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 any applicable policies or laws have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs of **MDM**. Such restriction is subject to **MDM** procedures or, in the absence of such procedures, to the approval of the employee's manager, or higher level management or the ITO

5.5.1 Methods of Connecting to the Internet

To ensure security and the spread of viruses and other security threats, Users accessing the Internet through a computer attached to the computer network of **MDM** must do so through the Internet Proxy Server of the Municipality or other information security systems like firewalls, Intrusion Prevention Systems, etc., put in place. Every employee will use his or her network username and password to access the internet for accountability and reporting purposes.

Bypassing computer network security of **MDM** by accessing the Internet directly by modem, 3G modems and mobile phones connected to computers, non-Municipality wireless networks or other means is strictly prohibited unless the computer you are using is not connected to **MDM** computer network and the method you are using has been supplied or sanctioned by the Municipality. Disabling of or subverting any security software installed on Municipality computers shall also constitute breach of this policy.

5.5.2 Detection of Viruses

Files obtained from sources outside **MDM**, 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 **MDM** computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-**MDM** sources, without first scanning the material with **MDM**-approved virus and malware protection software. If you suspect that a virus has been introduced into

MDM computer network, employees are required to notify ITO immediately. If you are not certain on how to scan for viruses immediately contact ITO for assistance.

5.5.3 External Email Accounts and Instant Messages

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 disclosure of sensitive official information. Only Municipality 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, Skype, etc., users are not allowed to be use and/or install any instant messaging application on Municipality computers or networks.

5.5.4 Distribution of Information and Data

Without prior written permission from **MDM**, the computer network of **MDM** 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 performance of **MDM** network or I.T infrastructure;
c) violate any other policies, provisions, guidelines or standards of this policy or any other of policies **MDM**;

Further, at all times users are responsible for the professional, ethical and lawful use of the Municipality internet facilities.

5.5.5 Communication of Official Information

Unless expressly authorized to do so by the accounting officer, users are prohibited from sending, transmitting, or otherwise distributing official information, data or other sensitive/confidential information belonging to **MDM** 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.

5.5.6 Discussion Groups

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

5.5.7 Copyright Restrictions

Users may not illegally copy material protected under national and international copyright laws or distribute that material to other users or people within or outside **MDM**. Users are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material they 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 Municipality.

5.5.8 Frivolous Use

Computers, computers networks and IT 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, users 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.

Furthermore, every user will be allocated a finite amount of data cap of internet traffic to be determined by ITO and approved by the Accounting Officer or his delegated authority. If a user exceeds this limit, his or her internet access will be revoked and re-enabled the next day. This quota limit does not apply to authorized ITO employees who are required to download large files for purposes of computer and network supports functions. A user who requires a higher daily limit for official purposes must send seek permission from their manager through a memorandum, clearly stating the reasons for the request. Such requests will be granted or declined on their individual merits at the discretion of ITO after assessing its impact on the network, bandwidth and internet service of the Municipality.

5.5.9 Limitation of Privacy

Employees are given computers and Internet access to assist them in the performance of their official duties. 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 internet facilities of **MDM**.

User consents to allow ITO or management of **MDM** to access and review of all materials created, stored, sent or received by users through Municipality Internet facilities for the purposes of accounting, monitoring of policy compliance and internet usage statistics.

5.5.10 Discriminatory, harassing and/or offensive language

Users are to refrain from using obscene, defamatory, derogatory, discriminatory or any offensive language while using internet facilities of **MDM** as such actions could have serious criminal, civil and moral consequences. This undesired and disallowed behavior may also constitute bridge of other MDM policies or laws of the country, and as such, users may be held liable for such bridges.

5.5.11 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 malware 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 ITO. A user knowingly downloads and installs any software from the internet that can compromise the MDM computer network, information systems or other users will be in violation of this policy.

5.5.12 Additional connection to the Internet

The Municipality offers additional tools, like 3G modem, 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 modems are governed by this Internet Acceptable Use Policy and as such 3G modem users must ensure that they utilize these 3G modems for official purposes. 3G modem users are more vulnerable to virus attacks and other security risks from the internet as they are not protected by the municipality information security systems. This means that 3G modem users visiting malicious sites could unknowingly distribute security risks to other computers while connected to **MDM** computer network.

To exercise control over security risks and maintain a single point of internet connection, all users connected to **MDM** computer network are not allowed to connect their 3G modems. Additionally, the use of 3G modems applies only to users at remote locations. 3G modems are only intended for internet access and they shall not be used for any other purposes like making phone calls or short message services. In the instance that a 3G modem user uses the 3G modem for making phones calls, the user shall be liable for any costs incurred and may be subject to disciplinary actions and/or revoking of the 3G modem.

No internet user is allowed to configure or enable other connections to the internet via modems, wireless networks and cellular telephones on Municipality computers. Any additional internet connections should be reported to the ITO.

5.5.13 Monitoring and Reporting

MDM 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 Municipality. In addition, all of the Municipality's Internet facilities are provided primarily for official purposes. Therefore, the Municipality 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 ITO 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 the Accounting Officer for purposes determined by the Accounting Officer or to enable ITO to properly implement systems that will cater for the future growth demands and to ensure on-going availability, scalability and reliability of these systems.

5.5.14 Prohibited Use

- Accessing streaming audio or video, play online games;
- Accessing chat sites;
- Installing and using instant messaging applications;
- Download of copyrighted material including videos, music, software or any intellectual property
- 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.;
- 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.
- Using the internet to conduct criminal or fraudulent activities;
- Using the internet to illegally monitor, gather information about any individual, entity or organization;
- Using the internet to intentionally subvert security systems or initiate a denial of service against any information system or network;
- Using the internet to conduct any personal business operations at the expense of the Municipality's bandwidth and resources;
- Connecting to the internet via 3G while the computer or laptop is connected to the Municipality network.
- Using the internet such that it interferes with employee productivity
- Sharing of usernames and passwords used to access the internet with other people including employees
- Distributing of passwords or any sensitive user account information through the internet
- Impersonating, misrepresenting or suppressing a user's identity when accessing the internet
- Using 3G modems for making telephone calls or sending SMS
- Using the Municipality internet facilities to intercept or disclose, or assist in intercepting or disclosing electronic data or information.
- Accessing P2P networks and web sites
- Using profanity, obscenities or derogatory, sexist, racist, highly sensitive, offensive or defamatory remarks while using the internet.
- Using the internet to access malicious sites and download illegal material
- Use of VoIP applications not necessary for official duties.

5.5.15 Conditions for Internet Access

A user must accept and sign 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, including, and not limited to revoking the user's internet access and/or disciplinary action in accordance with applicable policies and procedures of **MDM** 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.

5.5.16 Authorization Procedures

For purposes of ensuring proper use accountability, control and proper use of the Internet, every employee utilizing a Municipality laptop, computer, and/or 3G modem shall sign on the Internet Acceptable Use Undertaking (**IAUU**) in **Annexure A,** through which, he/she will abide by the policy stipulations contained in this policy. This signed undertaking will be kept in the user's personnel file, and a copy will be kept by the ITO. The signed undertaking will be filled in the staff file of the employee. The ITO and HR Office will take all steps to ensure that all the employees are provided with these undertaking and that they are signed by all employees. Failure to sign the IAUU will lead to existing internet access for the concerned user revoked.

In addition to signing the undertaking, a network logon message will be presented through which an employee will further agree to abide by the provisions and aspects of this policy and any other relevant policies related to use of MDM computers, computer networks, and all other I.T resources.. This logon message will clearly indicate where the user can locate the policies for review. At this point the user will also be presented with an option to either agree to the policies by clicking the **OK** button or disagree by clicking the cancel button. Computers, computer network and all I.T resources will not be available to any user who does not agree to abide by and be legally bound by the all IT policies and any other MDM policies and laws of the country related to computer use.

5.5.17 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 I.T Manager 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 individuals and ensure that they fully acknowledge this privacy concern.

5.5.18 Consequences of Non-Compliance

All **MDM** employees, users, contractors or temporary staff who have been granted the right to use the Internet access of **MDM** are required to sign Internet Acceptable Use Undertaking, confirming their understanding and acceptance of this policy. All MDMD employees, users contractors or temporary staff who have been granted the right to use the Municipality's Internet facilities are also required to accept and sign all other I.T Policies of **MDM**. As already stated, non-compliance to this policy may lead to disciplinary actions, legal liability as well as internet privileges for the user in violation revoked.

5.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "Electronic Mail Policy". These duties include, but are not limited to:

- Investigation of alleged or suspected non-compliance with the provisions of this policy; and
- Suspension of service to users, with or without notice, when deemed necessary for the operation and/or integrity of the Municipality's communications infrastructure, connected networks, or data.
- The ITO is able and reserves the right to monitor and/or log all network activity without notice, including all e-mail and Internet communications. Therefore, users should have no reasonable expectation of privacy in the use of these resources.
- While the **MDM** will not regularly monitor internet usage, users are on notice that the maintenance and operations of Internet Proxies and Firewalls may result in observation of internet activities and history. Internet browsing and usage is neither personal nor private.
- However, management and technical staff may monitor:

- for a legitimate business purpose (e.g. the need to access information when a user is absent for an extended period of time);
- To diagnose and resolve technical problems involving system hardware, software or communications; and/or to investigate possible misuse of internet facilities when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.
- By participating in the use of networks and systems provided by the **MDM**, users agree to be subject to and abide by policies governing their usage. **MDM** management will review alleged violations of this policy on a case-by-case basis.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal. Disciplinary action will be applied in a progressive manner in line with the applicable agreements concluded with organised labour or any such applicable policies of **MDM**.

5.7 COMMENCEMENT AND REVISONS

This policy takes effect from the date of its adoption by a council sitting or as shall be determined by council as shall be indicated in the council resolution and will be reviewed annually. The policy may be amended from time to time. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on municipality Intranet or website and/or by way of e-mail.

6. SOFTWARE INSTALLATION POLICY

6.1 INTRODUCTION

Installation of unauthorized computer programs and software, including files downloaded and accessed from the internet, can easily and quickly introduce serious, fast-spreading security vulnerabilities on the Mopani District Municipality's Information Technology Systems. Unauthorized software programs, even those seemingly provided by reputable vendors and trusted companies, can introduce viruses and Trojan programs that aid hackers' attempts to illegally obtain sensitive, proprietary and confidential data. Protecting the organization's computers, systems, data and communications from unauthorized access and guarding against data loss is of paramount importance; adherence to the following Software Installation Policy serves a critical role in the process.

6.2 BACKGROUND

The purpose of this policy is to ensure that every employee, contractor, temporary and volunteer understands, and agrees to abide by, specific guidelines for software, program and application installation and use on computers, systems and networks provided by Mopani District Municipality (MDM) for purpose of doing their work.

6.3 PURPOSE OF THE POLICY

The purpose of this policy is to establish guidelines, define users' roles and responsibilities as well as minimum requirements governing installation of software on computers provided to users by **MDM**. This policy specifically pertains to installation and removal of software on MDM systems. By establishing and maintaining compliance with this policy, risks and costs to the Municipality can be reduced while the valuable potential of all proprietary software would be is realized. The objectives of this policy are to assure that:

- The installation and use of computer software provided by **MDM** is related to, or for the benefit of the **MDM.**
- The installation and use of computer software contribute to the accomplishment of officials duties
- Users understand that installation and use of computer software is subject to the same laws, regulations, policies, and other requirements as information manipulated, stored, and communicated by the software.
- Disruptions to **MDM** activities from inappropriate installation and use of computer software provided by the Municipality are avoided
- Users are provided with guidelines describing their personal responsibilities regarding software installed on **MDM** information systems.
- Potential risk to sensitive systems and/or information is minimized to acceptable level.

6.4 POLICY SCOPE

The scope of the policy covers those people who make use of MDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "USERS". Users are all permanent, contract and temporary personnel employed by the **MDM** who have been issued with a Municipality's Computer or access to **MDM** information systems.

This policy refers to "Users" as all computer users at the MDM, whether they are permanent, on contract or temporary employees supplied by service-providers to the Municipality.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the Municipality's computers.

6.5 POLICY STATEMENT

6.5.1 Approved Software Applications

The Information Technology Office (ITO) tests and approves the use of only specific software programs and applications, including updates and patches to existing installed applications.

Only the information technology department will install approved software programs, applications and updates on all **MDM** systems and for those users requiring those programs and applications.

The installation and use of any unauthorized applications is prohibited.

Employees and other users must obtain written approval from **ITO** prior to requesting any unauthorized software or using any unapproved application on any information technology equipment or systems provided by **MDM**, with the exception of the following software applications:

- Adobe Acrobat Reader.
- Mozilla Firefox Web Browser.
- OpenOffice.org Office Suite.
- Spigot Search & Destroy.

6.5.2 Prohibited Software

Mopani District Municipality's computer systems, networks and information technology services are provided as a means of fulfilling job tasks and responsibilities. Mopani District Municipality places a priority on ensuring all installed software and applications are properly tested and licensed. Users are prohibited from installing any software programs and applications (other than those expressly listed in the Approved Software Applications section), including software purchased for personal use. Under no circumstances are users to download, install, copy, access, execute or otherwise employ any of the following:

- Illegal software or programs.
- Unlicensed applications.
- Unapproved or unlicensed operating systems.
- Pirated software.
- Software purchased for personal or home use.

6.5.3 Installation of Software

6.5.3.1 Installation of MDM Purchased Software on Personal Computers

IT staff will not install software or copy data files on personally owned computers.

MDM retains the rights of ownership for any MDM purchased software media, and will only provide checkout media for home installations where allowed by EULA.

Individuals that have installed MDM purchased software on their personally-owned computers are responsible for abiding by the EULA (End User License Agreement) agreement (which may include removal of the software upon termination of employment).

6.5.3.2 Installation of Personally Purchased Software on MDM Owned Computers

The **ITO** staff will not install personally- owned or purchased software or data files on MDM owned computers;

When MDM owned computers are replaced, it is the user's responsibility to make any copies of personally-owned software and data files before the old computer is replaced, and their responsibility to re-install such software on the new computer. The **ITO** staff will gladly assist, though the responsibility remains with the user concerned;

Users installing personally purchased software on **MDM** owned computers must provide **ITO** staff the EULA for each software package, prior to its installation. **ITO** staff will evaluate and verify compliance of the software license agreement. In many cases, license agreements may require the package to be removed from home microcomputers (may not be used on more than one CPU).

6.5.3.3 Installation media of all software purchased by MDM

IT staff will retain the installation media of all software purchased by the Municipality;

In cases where other departments/directorates staff do installations of database access software, the department/directorate or concerned departments will retain an installation copy of the media and will make copy for ITO.

6.5.4 Responsibilities of ITO Staff

ITO staff will install all software purchased by the Municipality, but only on Municipality owned computers.

All software installed on **MDM** owned systems must be accounted for through some form of proof of purchases and copies of **EULA** agreements (this includes personally owned software).

ITO staff will perform periodic audits to ensure software compliancy. Proof of purchases and copies of **EULA** agreements are required pieces of evidence towards compliancy.

ITO staff will perform migration of programs and data from one **MDM** owned computer to a replacement unit owned by the municipally. This may occur when a unit either becomes non-repairable, becomes obsolete, or through periodic replacement plans.

ITO staff will retain a copy of the hard drive image for no more than 30 days after a system migration has been performed. It is the responsibility of the user to ensure they have the appropriate and legal software/data on their system backed up to either their H: (network home folder for each user, located on the file server) or alternative media (CD/DVD/USB flash-drive).

6.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "Software Installation Policy". These duties include, but are not limited to:

- The **ITO** is responsible for enforcing this policy and continuously ensuring monitoring and compliance to this policy, including, but not limited to, compliance to EULA's of various software.

- The ITO will also monitor installation and use of software purchased by MDM to ensure maximum Return on Investment (ROI).

- Investigation of alleged or suspected non-compliance with the provisions of this policy; and

- Suspension of service to users, with or without notice, when deemed necessary for the operation and/or integrity of the Municipality's communications infrastructure, connected networks, or data.

- The **ITO** is able and reserves the right to monitor and/or log all network activity without notice, including all system applications and software, e-mail and Internet communications. Therefore, users should have no reasonable expectation of privacy in the use of these resources.

- In application and enforcement of this policy, **MDM** or designated staff within ITO may regularly access users' systems and/or electronic mail, and users are on notice that the maintenance and operations of information systems may result in observation of random messages. E-mail messages are not personal and private and are regulated by the Electronic Mail Policy and all other applicable policies, regulations, and laws. E-mail system administrators will not routinely monitor individual staff member's e-mail and will take reasonable precautions to protect the privacy of e-mail.

- However, management and technical staff may access a user's e-mail:

  - ✓ for a legitimate business purpose (e.g. the need to access information when a user is absent for an extended period of time);
  - ✓ To diagnose and resolve technical problems involving system hardware, software or communications; and/or to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.
  - ✓ By participating in the use of networks and systems provided by the **MDM**, users agree to be subject to and abide by policies governing their usage. **MDM** management will review alleged violations of this policy on a case-by-case basis.

6.7 COMMENCEMENT AND REVISION

This policy takes effect from the date of its adoption by a council sitting or as shall be determined by council as shall be indicated in the council resolution and will be reviewed annually. The policy may be amended from time to time. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on municipality Intranet or website and/or by way of e-mail.

7. DATA CENTRE ACCESS CONTROL POLICY

7.1 INTRODUCTION

Data Centres are found in almost all organisations ICT infrastructure. These data centres host the server environment and electronic data. Due to the sensitivity nature of these data centres, a policy is imperative to guide Mopani District Municipality on the proper mechanisms to manage this room as well to protect information.

7.2 BACKGROUND

The vulnerability of business critical information systems and the data they contain within the Data Centre make the site a high value asset, which requires a high degree of protection.

A range of security measures are therefore in place to protect employees, information and physical assets, along with the reputation of MUNICIPALITY NAME and interested third parties with equipment in the Data Centre.

7.3 PURPOSE OF THE POLICY

The purpose of this document is to define the policies and procedures relating to access control, environmental control, and operations of Mopani District Municipality Data Centres.

7.4 SCOPE OF THE POLICY

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

- Security
- Safety measures and procedures
- Emergency measures and procedures
- Access control procedures
- Change and configuration management
- Environmental control, reporting and maintenance
- Facilities Monitoring.

7.5 POLICY STATEMENT

7.5.1 SECURITY

7.5.1.1 Entry Systems and Access Control

Access shall be controlled via Biometrics fingerprint system and all doors shall be fitted with sensors to detect unauthorised or prolonged opening.

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 ITO.

Any person requiring access to the Data Centre shall sign the log book located on the desk of the Secretary to the Municipal Manager, located on the second floor of the Main Office in Giyani or at the receptionist at the Mopani Disaster Management Centre in Tzaneen

Only authorised ITO personnel 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 ITO personnel and/or Security personnel during office hours.

Tailgating into restricted areas is prohibited. Care shall therefore be taken by all authorised staff to prevent this. During deliveries, authorised staff shall supervise such work at all times.

7.5.1.2 Contractor Access After Working Hours

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

In case where contractors require access to Data Centre after hours, Security Services shall be responsible to provide such access and protection.

The Assistant Director for Information Technology will authorise the use and changes to be made in the Data Centre

7.5.1.3 Close Circuit Television

Internal, entry and exits areas of the Data Centre shall be monitored by a closed circuit television (CCTV) to capture all Data Centre activities.

CCTV shall be integrated and monitored by Security Services.

7.5.2 SAFETY

7.5.2.1 Overview

In addition to the safety precautions outlined herein, the Data Centre safety precautions shall be applied in conjunction with Mopani District Municipality Occupational Health and Safety policy and any statutory laws applicable in matters of Occupational Health and Safety.

7.5.2.2 Signs and Information

Safety signs and information shall be posted at access points to the Data Centre.

General notices shall also be posted around the Data Centre; providing detailed information on first aid, emergency contacts and general Health and Safety issues

7.5.2.3 Health and Safety Considerations

- No one should attempt to lift heavy equipment without suitable help.
- No one should attempt to lift equipment in and out of racks unaided, particularly where height makes the task more dangerous.
- Noise levels shall be checked at every half-year to ensure a safe working environment.
- Ear defenders shall be made available and be worn if working in the Data Centre for periods longer than 30 minutes.
- Anyone working in the Data Centre for prolonged periods should let staff know of their presence. Users are advised to take regular breaks from working to avoid adverse effects from temperature and noise levels in particular.
- Flexible safety barriers shall be available and be used to lift up raised floor tiles.

7.5.2.4 Emergency Exits and Fire Alarm Procedures

When fire alarm is triggered at the Data Centre, normal emergency procedures shall be followed as stipulated by Mopani District Municipality emergency evacuation procedures. Lifts shall not be used; only emergency stair ways shall be used.

7.5.2.5 Fire Detection and Fire Extinguishers

Fire and smoke detection system shall be fitted and linked to audible and virtual alarms.

If an alarm is activated the Data Centre shall be evacuated immediately to avoid gas inhalation and the incident shall be reported to Security Services and or ITO.

7.5.2.6 Electrical Safety

Only qualified electrical technicians shall have access to electrical systems, IT staff and other personnel should contact the relevant electrical personnel when encountering electricity problems.

Request shall be authorised by the Assistant Director for Information Technology.

7.5.3 DATA CENTRE USE

7.5.3.1 Hours of Operation

The Data Centre will be operated during office hours of Mopani District Municipality to authorised personnel between 08:00 am and 16:30 pm.

Access outside office hours for maintenance purposes will be authorised and delegated by the Assistant Director for Information Technology.

7.5.3.2 Equipment Delivery

Delivery of equipment shall be supervised by authorised personnel upon approval by the

Assistant Director for Information Technology.

7.5.3.3 Control of Equipment and Spares

No unused equipment and spares shall be left at the Data Centre.

Alternate storage facility shall be made available for such purpose.

7.5.3.4 Prohibited Items

The following items are prohibited from the Data Centre:

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

7.5.3.5 Cables and Wiring

Cables and wires shall be structured and labelled when running under the raised floor, wall, and equipment racks.

7.5.4 ENVIRONMENT

7.5.4.1 Air Conditioning

Under floor air conditioning shall be provided in the Data Centre. It shall deliver enough cooling per rack in accordance with design specification.

Service shall be done at least three times a year by a reputable maintenance service provider for air conditioning equipment installed in the Data Centre. Certificate for maintenance performed shall be submitted to the ITO.

7.5.4.2 CO2 Fire Extinguisher

Class E gas fire extinguisher shall be implemented to prevent damage to Data Centre electrical facilities.

Service shall be done at least once per annum by a reputable maintenance service provider for CO2 gas. Certificate for maintenance performed shall be submitted to ITO.

7.5.4.3 Power and Lighting Provisioning

Two single phase power sockets shall be available in each rack and shall be fed directly from the main distribution board.

Adequate power light shall be available to ensure that all equipment in the Data Centre is clearly visible.

Lights shall be switched off when no access to the Data Centre is required.

7.5.4.4 UPS Provisioning

All major equipment at the Data Centre shall be powered on by a UPS system, should the AC power goes down. The UPS system should sustain power to those devices for at least 5 minutes to allow graceful shutdown.

Service shall be done at least annually by a reputable maintenance service provider for UPS equipment fitted in the Data Centre. Certificate for maintenance performed shall be submitted to the ITO.

7.5.4.5 Temperature and Humidity

Temperature and Humidity monitoring devices shall be implemented and set to monitor deviations against baseline set according to standard set by ITO as recommended by Information and Communication Technology Industry Best Practices and Standards.

7.5.4.6 Environment Monitoring

A number of monitors shall be put in place to report on issues affecting the Data Centre environment.

Monitoring system shall report to designated ITO and Security personnel.

Monitoring shall include:

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

Maintenance Service shall be done at least twice per annum by a reputable maintenance service provider for equipment installed in the Data Centre. Certificate for maintenance performed shall be submitted to the Department.

7.5.4.7 Dust Prevention

The Data Centre shall be well ventilated to prevent dust from affecting equipment.

Equipment to be installed in the Data Centre shall be free of dust before being introduced in the Data Centre.

7.5.4.8 Disposal and Cleaning

Cardboard and other items that can generate dust and that are easily combustible should remain outside the Data Centre.

Waste bin shall be available outside the Data Centre main entrance for easy disposal of other items of waste.

7.5.5 CHANGE AND CONFIGURATION MANAGEMENT

The Assistant Director for Information Technology is responsible for all changes that shall take place at the Data Centre.

All changes to be made shall be requested to and authorised by the Assistant Director for Information Technology.

All changes to be made to the Data Centre will be done in accordance with Change Management Policy of Mopani District Municipality.

The Assistant Director for Information Technology will monitor and review the Data Centre access log book on a regular basis.

7.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this policy. These duties include, but are not limited to:

- Investigation of alleged or suspected non-compliance with the provisions of this policy; and
- Suspension of access to the Data Centres for authorised personnel, with or without notice, when deemed necessary for the operation, security and/or integrity of the Municipality's Data Centres.
- The ITO is able and reserves the right to monitor and/or log all access to the Data Centres.
- Non-compliance to and/or violations of this policy may lead to disciplinary actions, legal liability, and/ or dismissal from employment of Mopani District Municipality.

7.7 COMMENCEMENT AND REVISION

The policy may be amended from time to time as deemed necessary to address gaps identified during its implementation. Such amendments shall, as soon as reasonably possible, be brought to the attention of all affected authorised personnel with access to the Data Centres , including by posting such amendments on municipality Intranet or website and/or by way of e-mail. This policy shall also be reviewed annually.

8. IT CHANGE MANAGEMENT POLICY

8.1 INTRODUCTION

The complexity of current business environments, and the diverse technology used in ICT infrastructure environments demands a greater control to minimize risk and potential impact on the business.

Procedures should be instituted to ensure all changes are recorded, followed up and escalated to management when necessary. It is important that these procedures are adhered to at all times.

8.2 BACKGROUND

Information Technology Change Management (Change Management) is the process that ensures the prompt and efficient handing of all changes to the information technology (IT) infrastructure. This is accomplished through the use of standardized methods and procedures that draw upon industry best practices.

It is important that changes to the computing environment are executed in a controlled manner in order to mitigate the risk of interruptions to service during prime access hours and in order to maintain a repository of knowledge about the current configuration and status of the computing environment.
This document defines the policies and procedures that the Information and Technology Office of Mopani District will use to control changes to the computing environment.

The main goal of IT Change Management is to accomplish changes in the most efficient manner while minimizing the impact to the municipality, costs, and risks.

8.3 PURPOSE OF THE POLICY

The purpose of this policy is to provide the Mopani District Municipality with a procedure for the change control function that shall be established to manage, record and track all changes for Mopani District Municipality IT environment.

8.4 SCOPE OF THE POLICY

The scope of the policy covers those people who make use of MDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "USERS". Users are all permanent, contract and temporary personnel employed by the **MDM** who have been issued with a Municipality's Computer.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the Municipality's computers.

8.5 POLICY STATEMENT

8.5.1 Process Overview

The Change Management Process seeks to manage and control the changes through processes and procedures and then ensuring that the appropriate authority levels exist for each change.

The following process steps shall be used within Mopani District Municipality:

8.5.1.1 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.

(c) Project related activities.

(d) Ad-hoc activities that influence service delivery.

8.5.1.2 Change Planning and Building

Under the responsibility of change planning and building, changes may be scheduled and planning may be provided if necessary for the optimum control of the change.

Change Management has a coordination role, supported by line management, to ensure that activities are both resources and also completed according to schedule.

8.5.1.3 Change Logging and Filtering

Under the responsibility of the IT Help Desk, changes are logged on the IT Web HelpDesk system.

Each Change may be categorized accordingly in the automatic function of the IT Web HelpDesk system.

A Request for Change Form (Annexure E) needs to be completed for the following changes to the ICT environment:

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

Table 5.1

There are two change types that have to be adhered to, on the basis of the above classes and items:

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

Table 5.2

8.5.1.4 Emergency Changes

The emergency change management process shall provide a change control mechanism in the event of an emergency. The goal is not to bypass the Change Management Processes but rather to speed up the process and execute it quickly and efficiently when the normal process cannot be followed due to an emergency.

The following criteria shall be accepted as Emergency Changes:

(a) Production loss

(b) Financial loss

(c) Prevention of death

(d) Legislation changes

8.5.2 Change Approval

Prior to the approval of changes, an approval indicator shall be allocated to the change to enable the correct workflow associated with the required approval. The risks of the change will determine the required approval:

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

Table 5.3

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

Table 5.4

The risk factor indicates the nature of the approval:

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

Table 5.5

8.5.3 Change Implementation

ITO shall be responsible for implementation of all changes as scheduled.

Feedback regarding the success or failure of the change shall be provided to the CMB within 7 working days after the planned completion time as, and is to be captured on the IT Change Request Form (Annexure E).

8.5.4 Change Review and Reporting

ITO management shall perform an evaluation of the changes implemented. The purpose of this review shall be:

- Establish if the change had the desire effect and met the objectives
- Tasks and follow-up actions assigned to correct any problems or inefficiencies arising in the change management process itself as a result of ineffective changes
- Where resources were used to implemented the change as planned, and any problems or discrepancies fed back to CMB helping to improve the future estimating process
- Review satisfactory and abandoned changed, and formally closes them in the ICT help desk system.

8.5.5 Communication

Communication will be managed according to the predefined communication structure for each project.

Communication shall include:

- Change approvals
- Change notifications
- Change control escalations
- Change management processes and procedure changes
- Change management standard changes
- Change management policy changes.

8.5.6 Roles and Responsibilities

Different owners of processes and responsibilities can be identified.

8.5.6.1 Assistant Director: Information Technology

The Assistant Director for Information Technology shall be responsible for:

- Defining of the Change Management process, procedure, division of work and the roles and responsibilities within the process
- Contributing to the evaluation or establishment of the change management system, ensuring conformance to documentation standards
- Maintaining the change management system in accordance with agreed procedures
- Reviews on procedures and other processes checking for compliance against the quality system, and external standards where appropriate
- Communicating all updates and/or changes of the Change Management Process
- Promoting awareness of the importance of a structured change management process, working with other business units

8.5.6.2 Change Management Board

The Municipality shall formulate a Change Management Board to function within the following mandate:

- To formalize an official forum to review all changes in a structured way.
- To focus the attention of the Committee to the management of changes.

The Change Management Board shall:

- Review all high impact changes to be implemented
- Review any change that was implemented unsuccessfully or had to be cancelled
- Screen all the changes to ensure the correct category, type and item have been selected.

- Monitor routine and low impact changes.

8.5.6.3 **ITO**

- Implement Change requests as per above mentioned Change Management Process
- Provide regular feedback on progress regarding the change request and schedule.

8.5.7 Change Lead Times

Change lead time is the amount of time required to evaluate and adequately plan for change implementation. Lead time is measured from the time the change is submitted until the change is actually implemented. Lead time shall vary by the type of change.

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	

Table 5.6

8.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "IT Change Management Policy". These duties include, but are not limited to Investigation of alleged or suspected non-compliance with the provisions of this policy.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action

will be applied in a progressive manner in line with the Memorandum of understanding on Conduct of Service 0f 1994.

Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

8.7 COMMENCEMENT AND REVISION

This policy takes effect from the date of its adoption by a council sitting or as shall be determined by council as shall be indicated in the council resolution and will be reviewed annually. The policy may be amended from time to time. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on municipality Intranet or website and/or by way of e-mail.

9. FIREWALL POLICY

9.1 INTRODUCTION

This document details the procedures undertaken during the operation of the Mopani District Municipality Firewall and details the requirements involved in securing the Trust Network Facilities through the use of a firewall.

9.2 BACKGROUND

A Firewall is a system designed to prevent unauthorised access to or from a private network through protecting and controlling both internal and external connections. Firewalls are an essential component of MDM's information systems security infrastructure. They are designed to establish a perimeter where access controls are enforced, thus enhancing security of computer and network resources to ensure a more reliable network and reduce illegal and malicious activities.

9.3 PURPOSE OF THE POLICY

The purpose of this policy is to ensure that the Mopani District Municipality (**MDM**) has the proper network perimeter security in place to prevent malicious intrusion while allowing communications necessary to facilitate daily municipality needs. Furthermore, this policy is designed to help protect electronic information systems and ensure compliance with other **MDM** policies, regulations, laws of the Republic of South Africa and best industry practices and standards

The purpose of this policy is to establish guidelines, define users' roles and responsibilities as well as minimum requirements governing installation of software on computers provided to users by **MDM**. This policy specifically pertains to installation and removal of software on MDM systems. By establishing and maintaining compliance with this policy, risks and costs to the Municipality can be reduced while the valuable potential of all information systems and data residing on them would be is realized. The objectives of this policy are to assure that:

- The use of computer networks, systems, and resources provided by **MDM** is related to, or for the benefit of the **MDM.**
- The use of computer networks, systems, and resources contribute to the accomplishment of officials duties.
- Users understand that use of computer networks, systems, and resources is subject to the same laws, regulations, policies, and other requirements as information manipulated, stored, and communicated by them.
- Disruptions to **MDM** activities from inappropriate use of computer networks, systems, and resources provided by the Municipality are avoided
- Users are provided with guidelines describing their personal responsibilities regarding use of **MDM** information systems and networks.
- Potential risk to sensitive systems and/or information is minimized to acceptable level.

9.4 POLICY SCOPE

This municipality-wide policy governs all computer systems connecting to **MDM** networks. All such systems are subject to access rules imposed by the MDM perimeter firewall. These access controls are established to mitigate threats from the Internet while allowing network activities necessary in performance of the municipality mission.

The scope of the policy covers those people who make use of MDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "Users". Users are all permanent, contract and temporary personnel employed by the **MDM** who have been issued with a Municipality's Computer or access to **MDM** information systems.

This policy refers to "Users" as all computer users at the MDM, whether they are permanent, on contract or temporary employees supplied by service-providers to the Municipality.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the Municipality's computers.

9.5 POLICY STATEMENT

9.5.1 Change Procedures

Firewall changes have been deemed as business as usual (BAU) changes or standard agreed changes by the Change Management Board (CMB) and the following process must be followed:

1. Complete a Change Request Form (See Appendix 1)

2. Requested/required change must be assessed and approved by a senior member of the Network Team. This assessment will evaluate such areas as the potential impact upon other Network Devices and Network Services.

3. Change application must be either approved or rejected, providing justification for the change approval/rejection.

4. Change must be implemented at a time that will have the least impact upon normal Firewall/Network Operations.

All of the change procedures must be fully documented and authorized and retained by the **ITO**.

When an emergency change is required, then the procedures set out in IT Change Management Policy must be followed.

9.5.2 Firewall Security

The security of all the network devices may be addressed on two levels: the physical and the logical. These two aspects ensure that all devices are secure and that no unauthorised access is permitted.

9.5.2.1 Physical Security

The Firewall physical device is located in a secure area of the Trust premises. This location is restricted through the use of secure key codes and swipe cards. These areas may only be accessed by a restricted number of authorised staff.

The physical access to secure areas is operated in accordance with the access control measures and security of the municipality.

9.5.2.2 Logical Security

Access to the MDM Firewall is governed by password authentication in accordance with User Account and Password Management Policy, IT Security Policy and all other applicable policies, procedures and laws of the RSA. Only the Assistant Director responsible for **IT** and designated personnel within **ITO** are permitted access to the Firewall. Any changes to any firewall devices or system-bases firewall application(s) must be performed by either of the Assistant Director responsible for **IT** or designated personnel within **ITO** duly authorized to do so. No other member of staff of **MDM** is authorized or capable of accessing the Firewall.

9.5.3 Firewall Monitoring

Regular monitoring of the Firewall will occur so that the device is functioning properly. It will also ensure that the **MDM** network is being provided with the requisite protection as stipulated in Anti-virus Policy, Internet Acceptable Use Policy, Electronic Mail Policy, IT Security Policy, and all other applicable policies and laws, and industry best practices.

9.5.4 Suspicious Activity Monitoring

The Firewall will be continuously monitored for any suspicious activity occurring. This monitoring will enable the **ITO** to identify any possible threats arriving through the Firewall and enable swift response to potential dangers.

9.5.5 Log File Monitoring

Due to the nature and size of log files, it is accepted that regular monitoring is not always feasible. As such, monitoring of any Firewall logs will occur only under specific circumstances such as:

- An attempted intrusion
- Suspicious Inbound/Outbound activity
- On the request of the Municipal Manager, Director responsible for Corporate and Shared Services, IT Steering Committee, Management Committee, Auditors (both internal and external) for purposes of auditing, or the Audit Committee.

Such monitoring, done outside the normal course of operations of the **ITO**, shall be done on request made in writing to the **ITO**, and subject to approval of the Assistant Director responsible for Information Technology. These requests will not be unreasonably denied, nor will such requests be made or granted for frivolous purposes, or in contravention of any other policies of **MDM** and laws of the **RSA**.

9.5.6 Security Monitoring

The **ITO** will perform regular auditing of the Firewall to ensure that the integrity of said devices has not been compromised. Examples of this auditing will take the form of:

- Regularly auditing access to the firewall devices/application software to ensure that only authorised users have gained access;

- Monitoring the firewall devices/application software for any suspicious activity etc.

This list is not exhaustive.

9.5.7 Analysis

Information gathered from the monitoring of the Firewall will be utilised to assess such areas as security. This will enable the **ITO** to efficiently assess the performance of the firewall devices/application software and ensure that security is maintained.

9.5.8 Port Control

The Firewall will provide access to the **MDM** Network only through a restricted number of TCP/IP ports. Any port that is not used to provide a connection will be disabled to prevent unauthorised access and ensure the **MDM** computer network security is maintained.

9.5.8.1 Inbound Connections

Inbound connections are defined as connections originating from the outside and destined for the inside of the firewall.

By default the firewall will deny all inbound connections. Rules must be created to allow specific inbound connections as defined in the Exceptions to Default Firewall Rules.

9.5.8.2 Outbound Traffic

Outbound connections are defined as connections originating from the inside and destined for the outside of the firewall.

By default the firewall will deny all outgoing connections. Rules may be created to allow specific outbound connection as defined in the Exceptions to Default Firewall Rules.

9.5.9 Users Access Control and Authentication

Further to restrictions set by allowing or denying specific inbound connections or outbound traffic TCP/TP ports, ability to access these ports will also be set on a user authentication basis. This authentication method will be achieved through integration of the Firewall with the Microsoft Windows Active Directory and access will be determined through the IT Asset Management Policy, User Account and Password Management Policy, Password Policy, Internet Acceptable Use Policy, and all other applicable policies of the **MDM**.

9.5.10 Standard Network/Intranet/Internet Traffic Flow

The firewall configuration consists of three active interfaces.

The Mopani District Municipality Local Area Network (LAN) is attached to the Network Interface Port 1 (Internal). This is where the LAN interfaces with the internet connection and the wide area network of **MDM.**

The Wide Area Network (**WAN**), connecting all satellite offices and fire stations back to the main offices in Giyani, is connected to Interface Port 2 (WAN). Each interface has been assigned a numerical security level, and listed in the table below.

The Internet/Government Core Communication Network (**GCCN**), supplied by State Information Technology Agency (**SITA**), is connected to Interface Port 3 (External). This interface allows both **MDM** LAN and WAN to connect to the internet.

Table 1: Security Hierarchy

Level	Description	Interface
100	MDM LAN	Interface Port 1
50	MDM WAN	Interface Port 2
0	Internet/GCCN	Interface Port 3

By default all connection requests from a higher security level to a lower security level will be allowed. By default all connection requests from a lower security level to a higher security level will be denied. When connection requests from a lower security level to a higher security level are required to support the **MDM** mission, an access rule must be added to the firewall, subject to approval of a written request for exception from the standard default firewall access rules by Assistant Director for Information Technology.

9.5.11 Standard Protocols

Only secure network protocols shall be used to transfer non-public or sensitive data across the firewall. Any exception must be documented as to why a secure protocol is not being used and the anticipated date of conversion to a secure protocol.

Standard Accepted Protocols

- DNS
- FTP (for non-sensitive data only)
- HTTP (for non-sensitive data only)
- HTTPS
- POP3 (for non-sensitive data only)
- SMTP (for non-sensitive data only)

9.5.12 Exceptions to Default Firewall Rules

9.5.12.1 Documented Exceptions

All exceptions to the default firewall access rules shall be documented and maintained by the **ITO**.

Requests for exceptions to the default firewall access rules should be submitted in writing on the prescribed Firewall Exceptions Application Form to the Assistant Director of Information Technology. Requests should include the following information:

- Source IP Address
- Source Contact (Name, Phone, Email)
- Destination IP Address
- Destination protocol and port
- Destination Contact (Name, Phone, Email)
- Reason for requested exception (in support of **MDM** mission)
- Signature(s) of affected System / Data Owner(s)

Source and destination IP addresses and ports must be as specific as possible. This will maintain security by ensuring that only necessary systems and ports are accessible through the firewall.

9.5.12.2 Exceptions Review

All exceptions to the default firewall access rules shall be reviewed at least once per semester. Upon adding or removing a firewall access rule that affects a particular system, all firewall access rules affecting that system will be reviewed. Changes to major systems, including removal from the network, will trigger a review of all firewall access rules related to that system.

The purpose of the review will be to identify firewall access rules that need to be removed or further limited. If questions arise or a change is necessary, the system / data owner will be consulted. Any resultant changes will be documented and performed on the firewall.

9.5.13 Virtual Private Network (VPN) Access

Virtual Private Network (VPN) access allows a remote computer to have network access as if it on the **MDM** network and directly connected to the local area network. VPN access allows users to access the same network resources they use in the office from outside the office.

MDM employees that have a job-related reason to access restricted **MDM** systems from outside the premises of **MDM** may request VPN access to the **MDM** network. That request should be made in writing to the Assistant Director of Information Technology. VPN access will be limited to those employees and job-functions that will provide a benefit to the municipality by allowing access from outside the premises of **MDM**.

9.5.14 Enforcement of Firewall Access Policy

Firewall rules will be used to enforce the requirements set forth in this document. In the event of an emergency, additional configuration and procedural changes may be made in order to protect the MDM computer network. Management and staff will be informed immediately if these changes are significant or disruptive. Workarounds will be provided for any disrupted services.

In the event an acceptable workaround is unavailable, the Assistant Director of Information Technology, in consultation with the Director of Corporate & Shared Services and the Municipal Manager, will determine the course of action.

9.5.15 Roles and Responsibilities

The operational responsibility for the Firewall rests with the Assistant Director responsible for Information Technology and he may delegate such responsibility to any designated personnel with requisite skill and knowledge of the functioning of the Firewall within **ITO** while accountability will not transfer with such designation. The Assistant Director responsible for Information Technology may, from time to time, be required to report on matters related to the Firewall to higher offices and structures within **MDM**.

9.5.16 Monitoring and Auditing

The Information Technology Steering Committee is the **MDM** Committee with responsibility for the formulation of Information Technology Governance Framework (policies, procedures, plans, standards, etc.) and approval of work programmes for Information Technology within **MDM**. This committee should have senior level representation from all appropriate directorates to ensure the **MDM** implements this policy appropriately.

The Internal Audit Unit within **MDM** will periodically conduct baseline audit and construct/recommend action plans for future compliance with this policy and reduce risks to acceptable levels.

The Chief Risk Officer will maintain an IT risk register which is to be populated on the appropriate system/spreadsheet/database and it is the responsibility of all staff within the organisation to identify risks associated with IT within their arrears of operation.

The **ITO**, led by the Assistant Director for Information Technology, and assisted by the Director responsible for Corporate & Shared Services and the Municipal Manager, will play a lead role in implementation of this policy, and the process of identifying and managing risks associated with the use of information technology within MDM

9.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "Firewall Policy". These duties include, but are not limited to:

- The **ITO** is responsible for enforcing this policy and continuously ensuring monitoring and compliance to this policy, including, but not limited to, compliance to EULA's of various devices and software.
- Investigation of alleged or suspected non-compliance with the provisions of this policy; and
- Suspension of service to users, with or without notice, when deemed necessary for the operation and/or integrity of the **MDM** computer systems, communications infrastructure, connected networks, or data.
- The **ITO** is able and reserves the right to monitor and/or log all network activity without notice, including all system applications and software, e-mail and Internet communications. Therefore, users should have no reasonable expectation of privacy in the use of these resources.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the applicable human resource management policies and procedures. Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

9.7 COMMENCEMENT AND REVISIONS

This policy takes effect from the date determined by council in the resolution for its adoption, and will be reviewed annually or as the need arises, whichever comes first. The policy may be amended from time to time as the need arises. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on the Municipality Website or Intranet, or by way of e-mail or memorandum.

10. IT PATCH MANAGEMENT POLICY

10.1 INTRODUCTION

A rigorous patch management process is a fundamental security requirement for any municipality, and indeed any business, in operation today. Such a program ensures that the security vulnerabilities affecting municipality's information systems are addressed in an efficient, thoughtful, timely and effective manner. This process introduces a high degree of accountability and discipline to the task of discovering, analyzing and correcting security weaknesses in computer systems.

The patch management process is a critical element in protecting any organization against emerging computer security threats. Formalizing the deployment of security-related patches should be considered one of the key elements in ITO's program to enhance the safety of information systems for which they are responsible. The intent of this policy is to serve as a starting point for the municipality to practice secure patch management procedures.

10.2 BACKGROUND

Information security advisory services and technology vendors routinely report new defects in software. In many cases, these defects introduce opportunities to obtain unauthorized access to systems running this software. Information about security exposures often receives widespread publicity across the Internet, increasing awareness of software weaknesses, with the consequential risk that cyber criminals could attempt to use this knowledge to exploit vulnerable systems.

This widespread awareness leads vendors to quickly provide security patches so they can show a response to a vulnerability that has been publicized and avoid erosion of customers' confidence in their products.

Historically, most organizations tend to tolerate the existence of security vulnerabilities and, as a result, deployment of important security-related patches is often delayed. Most attention is usually directed toward patching Internet-facing computer systems, firewalls and servers, all of which are involved in data communications to business partners and customers. These preferences resulted from two fundamental assumptions:

- The threat of attack from insiders is less likely and more tolerable than the threat of attack from outsiders.
- A high degree of technical skill is required to successfully exploit vulnerabilities, making the probability of attack unlikely.

In the past, these assumptions made good, practical sense and were certainly cost-effective given the limited scope of computer systems. However, the threat profile and potential risks to an organization have both changed considerably over time.

Viruses can now be delivered through common entry points (such as e-mail attachments), automatically execute, and then search for exploitable vulnerabilities on other platforms. This was once just a theoretical threat, but became a reality with the release of the Nimda virus in September 2001.

With this in mind, the information technology department within an organization should develop a formal process to be used to address the increased threats represented by security vulnerabilities. This policy introduces and explains the elements of a security patch management process to meet the challenges vulnerabilities represent.

10.3 PURPOSE OF THE POLICY

- To create awareness across the municipality of the importance of patching all systems pro-actively.
- To provide a secure network environment for Mopani District Municipality automated applications, staff, business partners and contractors.
- To provide a resilient set of Information and Communication Technology resources that maintains acceptable and agreed levels of confidentiality, integrity and availability.
- To ensure that all computer devices connected to the Mopani District Municipality computer network have proper virus-protection software with current virus-definition libraries and the most recent approved operating system and security patches installed.

10.4 SCOPE OF THE POLICY

This policy applies to all computers used on the Mopani District Municipality computer network. This includes, but is not limited to, councillors, senior management, all staff, contractors and all their staff, agents, and partners, connecting their computers and computers networks to MDM computer network, and third party desktop and laptop computers. Computers that are not physically connected to the MDM network must also abide by this policy. Any exceptions to patch management requirements must be requested in writing (refer to Appendix A).

10.5 POLICY STATEMENT

10.5.1 General Principles

Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, approval, installing and verifying.

Automatic scanning systems, administered from central sites, are superior to manual patching methods and should be employed where possible. It must be possible to define scans by:

- IP ranges
- Domain/AD groups
- Machine Names

It must be possible to automatically deploy patches from central sites following the same criteria described in above for scanning.

If administrative rights to a computer are necessary requirements for a selected automated patch management system, then a local account should be created. Required administrative accounts will follow minimal password standards as laid out in the User Account and Password Management Policy and the Password Policy. Default passwords will not be allowed.

Patch management systems must be able to provide lists of:

- Missing Patches and/or Service Packs
- Software Versions
- Patches that were successfully applied
- Patches that could not be applied.

The patch management product deployed must store all information and data in a structured database.

All exceptions requests to this policy will be submitted in writing to ITO for approval and implementation, subject to recommendation of the head of the directorate owning the computer system. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions will be approved as interim in nature. ITO will monitor all approved exceptions.

10.5.2 Monitoring

The ITO will monitor security mailing lists, review vendor notifications and websites and research specific public websites for the release of new patches. Monitoring will include, but not be limited to, the following:

- Scanning MDM computer network
- Identifying and communicating known vulnerabilities and/or security breaches to the ICT Steering Committee
- Monitoring CERT, other advisories and websites of all vendors that have hardware or software operating on the MDM computer network.
- ITO will create and maintain and organisational hardware and software inventory and an electronic database of information on patches required and deployed on the systems or applications for the purposes of proper internal controls and reporting to the senior management and/or ICT Steering Committee.

10.5.3 Assessing and Classifying Risk

Once a new patch has been identified, the ITO will categorise its criticality relevant to each platform (for example, servers, desktops, printers and so on) according to the following:

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

If the ITO categorises a patch as an emergency, the municipality considers it as a threat to MDM computer network and systems.

10.5.4 Testing

- Once alerted to a new patch, ITO will download and review the new patch in line with the period defined within the risk matrix.
- ITO will assess the effect of the patch on the municipality information technology infrastructure prior to its deployment.
- Patches deemed Critical or Not Critical will undergo testing for each affected

platform before release for implementation. ITO will expedite testing for critical patches. The ITO must complete validation against all deployed system images prior to implementation.

- Patches will be tested on non-production systems prior to installation on all production systems.
- Once ITO is satisfied that the deployment of a new patch will not cause any unexpected behaviour, they must agree upon a schedule for deployment with the user department/directorate.
- It is the responsibility of application owners and/or users to identify any problem(s) with a patch(es) and to notify the ITO of the problem(s). Applications and their owners need to be defined and listed in the Configuration Management database.
- While ITO will assist in resolving incompatibility issues, it is also the responsibility of application owners to resolve this incompatibility with the application's manufacturer.
- If the manufacturer cannot resolve the incompatibility, the risk incurred by not patching the computer(s) in question must be weighed against the risk of not running the application.
- The Assistant Director for Information technology and the head of the application owner department/directorate, in consultation with the Chief Risk Officer, should evaluate the options taking into consideration the nature of the vulnerability, the likelihood of its exploitation and the impact to operations of application malfunction.
- If they determine that the patch in question should not be deployed, this decision must be documented for record purposes and possible reporting to ICT Steering Committee and/or Senior Management or higher structures.

10.5.5. Authorisation and Notification

- The Assistant Director for Information Technology must approve the schedule prior to implementation. Regardless of criticality, each patch release requires the creation and approval of a request for technical change (RTC) prior to releasing the patch. The Director for Corporate Services will decide when notifying staff is necessary.
- ITO will obtain authorisation for implementing Critical patches via an emergency RTC and CMB approval. The ITO will implement Not Critical patches during regularly scheduled preventive maintenance. Each patch will have an approved RTC. For new network devices, each platform will follow established hardening procedures to ensure the installation of the most recent patches.
- Since a security patch may cause a system to malfunction, departmental ITO should proactively announce the deployment of a patch(es).

10.5.6. Deployment

- Critical security patches should be deployed within five business days of the time the vendor makes them available.
- Non-critical security and other patches may be applied monthly.
- Emergency patches will be deployed within eight hours of availability. As Emergency patches pose an imminent threat to the network, the release may proceed testing.
- Patches that are not deployable with automated patch management solutions will be deployed manually within the timeframes and requirements laid out in this policy.
- In all instances, the user department/directorate will perform testing (either pre or post-implementation) and document it for auditing and tracking purposes.

10.5.7. Verification

- Post-patch audit scans must occur within one (1) week after the vendor releases a critical security patch.
- Audit reports must be maintained for at least one (1) year.
- ITO must perform regular or pre-patch network-wide audit scans on all systems and devices at least monthly.
- Following the release of all patches, ITO and user department will verify the successful installation of the patch and that there have been no adverse effects.
- All Patch Management Reports as prescribed in this policy will serve in the ICT Steering Committee meetings.

10.5.8. Contingency Planning

- A roaming workstation must have a patch management solution configured to automatically download and install approved patches when it physically connects to the MDM computer network.
- In the event that a critical patch cannot be centrally deployed, it must be installed in a timely manner either manually or via a vendor maintained update site.
- One or more alternate ITO staff must be designated and trained so that in the event the primary server administrator, or Assistant Director for Information Technology are not available the patch and audit processes can proceed normally.
- Copies of current patches will be maintained by ITO staff and stored in a secure location.

10.5.9. Responsibilities

10.5.9.1 Director: Corporate Services

- Support the establishment of departmental patch management policy and procedures within the MDM.
- Ensure that funding and personnel are provided to effectively maintain institution-wide patch management solutions.\

10.5.9.2 Information Technology Office (Assistant Director: IT)

- Ensure that all IT systems are patched in timely manner as laid out in this policy.
- Review current threats and vulnerabilities and to check relevant advisories to monitor any potential threats or vulnerabilities.
- Establish and implement a departmental program for patch management on all IT systems.
- Ensure that all IM&T staff, especially System and Network Administrators are trained and made aware of this policy and relevant procedures.
- Assign system administrators and other authorized personnel specific patch management and vulnerability correction responsibilities.
- Deploy the municipal or an approved automated patch management solution to facilitate compliance with this policy and to promote efficiency for all systems, wherever feasible, apply patch management solutions to in-house applications and monitor status of those systems.
- Ensure that a departmental inventory of hardware and software patch status is 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.
- Report patch management status monthly to the Information & Communication Technology Steering Committee using the Patch Management Compliance Form (see Appendix A).
- Request a formal exception through the established process for any systems which are not compliant within 90 days.

10.5.9.3 IT Security Officer

- Develop and publish policy and procedural guidance on patch management.
- Provide institution-wide tools to assist agencies in compliance efforts.
- Monitors patch management on a directorate/department-wide basis.
- Provide advice and guidance to directorate/departments in effectively patching systems and eliminating vulnerabilities.

- Support exception requests from the patch management policy to ensure that appropriate security protection is provided.

10. 5.9.4 ICT Steering Committee

- Members to proactively monitor their own departments/directorate IT resources for known threats and vulnerabilities through monitoring advisories and current best practice.
- To review all recommended patching requirements and to classify severity rating of patches in line with the agreed risk matrix (see Appendix B).
- Become familiar with the MDM Patch Management Policy, procedures, institution wide solutions and best practice.
- Act as a Point of Contact (POC) for information security to provide guidance and assistance to ITO officials designated patch management responsibilities.

10.5.9.4 All Staff and third parties contracted to MDM

- Must abide by this Patch Management Policy and all other applicable IT policies.
- Must report any suspected lack of compliance with this policy to the ITO. Failure to do so constitutes a violation of policy.

10.5.10 Mopani District Municipality

(i) Reserves the right to monitor for violations of this policy.

10.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "IT Patch Management Policy". These duties include, but are not limited to Investigation of alleged or suspected non-compliance with the provisions of this policy.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the Memorandum of understanding on Conduct of Service of 1994.

Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

10.7 COMMENCEMENT AND REVISION

This policy takes effect from the date determined by council in the resolution for its adoption, and will be reviewed annually or as the need arises, whichever comes first.

The policy may be amended from time to time as the need arises. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on the Municipality Website or Intranet, or by way of e-mail or memorandum.

11. ANTI-VIRUS POLICY

11.1 INTRODUCTION

This Anti-virus policy prescribes how viruses, adware and malware are to be handled on every computer 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. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

11.2 BACKGROUND

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event to computer software, data and/or the network. Viruses can be transmitted via email or instant messaging attachments, downloadable Internet files, removable storage media such as USB disks, flash disks and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Mopani District Municipality in terms of lost data, lost staff productivity, and/or lost reputation

11.3 PURPOSE OF THE POLICY

This policy is designed to protect the Municipality IT resources against intrusion by viruses and other malware.

The purpose of this policy is to provide instructions on measures that must be taken by all **MDM** users to help achieve effective virus detection and prevention.

Through this policy ITO will strive to

(i) Provide a Municipality computer network environment that is free from viruses, adware, and all other forms of malware,;

(ii) Establish base requirements that must be met by computers connected to the Mopani District Municipality network to ensure effective virus detection and prevention

(iii) Ensure the integrity, reliability, and good performance of University computing resources;

(iv) Ensure that users operates according to a minimum of safe computing practices;

(v) Ensure that the Municipality licensed anti-virus software is used for its intended purposes; and

(vi) Ensure that appropriate measures are in place to reasonably assure that this policy is honoured.

11.4 SCOPE OF THE POLICY

This policy applies to all computers that are connected to the Municipality network via a standard network connection, wireless connection, modem connection, Government Core Communication Network (GCCN) or virtual private network connection. This includes both **MDM** owned computers, those owned by companies or persons contracted to **MDM**, and personally-owned computers attached to the **MDM** network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

All employees, both permanent and contracted, and personnel of companies contracted to MDM requiring access to **MDM** computing facilities or **MDM** networks are subject to this policy and required to abide by it and all other policies and/or laws related to this policy at all times.

11.5 POLICY STATEMENT

(ii) Centrally provided virus protection software will be run on all MDM computers and on all computers connected to **MDM** computer network. Supporting guidelines and procedures will be defined and will be utilised by the ITO to implement this policy and ensure compliance.

(iii) All computers attached to the **MDM** computer network must run standard and supported anti-virus software. This anti-virus software must be active all the time and must be configured to perform on-access real-time checks on all executed files and scheduled virus checks at pre-set regular intervals. The virus definition files must be kept up to date all the time.

(iv) Currently, **MDM** standard anti-virus for Windows Operating System computers and servers is based on Symantec Endpoint Protection Suite anti-virus solution (see http://www.symantec.com for further details). Symantec Endpoint Protection agents are licensed and will be installed on every newly purchased Windows Operating System computer and/or Server.

(v) Any activity intended to create and/or distribute malicious programs onto the **MDM** computer network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.

(vi) If a user receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she must report such incident to the ITO immediately by e-mailing ito.helpdesk@mopani.gov.za. Report the following information (if known):

(a) Virus name,
(b) Extent of infection,
(c) Source of virus,
(d) Potential recipients of the infected material.

(vii) No employee should attempt to destroy or remove a virus, or any evidence of that virus, without directive and/or assistance from ITO.

(viii) Any virus-infected computer will be removed from the network until it is verified as virus-free.

(ix) Privately owned computers that are to be approved to connect onto MDM network or to process data intended for MDM use must be equipped with an appropriate anti-virus product in working order.

(x) Any activity intended to create and/or distribute malicious programs onto the University network (e.g. viruses, worms, Trojan horses, etc.) is strictly prohibited.

(xi) The University reserves the right to disconnect any machine from the network if an infection is found or suspected. The machine will be disconnected until the infection is removed.

(xii) Email attachments will be scanned by an anti-virus product.

(xiii) Scams and hoaxes: Many spam emails are sent about viruses with dire warnings or messages with topical subjects or attachments. Do not forward these messages on to all colleagues and friends. If you receive such a message, just delete it. If you want to check its validity, forward the message to the ITO on email address ithelpdesk@mopani.gov.za.

(xiv) Should users experience difficulties with the anti-virus product, requests for technical support must be forwarded to ITO.

(xv)

11.5.1 Guideline for Best Practices for Virus Prevention

(a) Always run the standard anti-virus software provided by MDM.

(b) Never open files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

(c) Never open files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.

(d) User accounts for temporary staff, contractors and service providers will be set to automatically expire on the last day of the contract. Should the contract be renewed, the user will be required to re-apply for network access. ITO will only re-enable the user account after receiving the new user application.

(e) 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.

(f) Passwords may not be blank.

(g) A password history of 20 passwords will automatically be stored by the authentication system and as a result users must not use previously used passwords when changing passwords.

(h) To prevent accidental disclosures of passwords and unauthorized access to newly created user accounts, initial passwords should be changed immediately within one day. Failure to do so will result in the newly created user account disabled after one day.

(i) User passwords must be changed every 42 days.

(j) Default system administrator accounts should be renamed and their passwords revealed on a need-to-know basis to authorized personnel only.

(k) No passwords will be stored in clear text or reversible encryption.

(l) The ITO 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.

(m) The least privilege principle will apply when creating new user account

(n) If a user's password has expired or the user has forgotten their password, then the user must complete a **Password Reset Request Form** and send it to ITO for processing. This is to ensure that all requests to reset passwords are recorded for auditing purposes and to prevent unauthorized resetting of other users' passwords. Assistant ITO may at their discretion require the user requesting the request to physically present himself/herself at the ITO.

(o) Passwords used within MDM should not be used for external internet accounts and service providers.

(p) Passwords must not be included in any automatic login process.

(q) New passwords may not resemble old passwords e.g. password1 and password2.

11.5.2 Exceptions

(i) Exceptions to this policy will only be granted if:

(a) Compliance would adversely affect the ability of the service to accomplish a mission critical function; or
(b) Compliance would have an adverse impact on the service provided or supported by the information, system or resource; or
(c) Compliance would have an adverse impact on the service provided or supported by the information, system or resource; or
(d) Compliance is achieved due the incapability of the information system or a resource.

(ii) A procedure for requests for exception to this policy will be produced and implemented

11.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "Anti-virus Policy". These duties include, but are not limited to:

- Investigation of alleged or suspected non-compliance with the provisions of this policy; and
- Suspension of service to users, with or without notice, when deemed necessary for the operation and/or integrity of the Municipality's communications infrastructure, connected networks, or data.
- The ITO is able and reserves the right to monitor and/or network logon activity without notice to monitor and brute forcing logon attempts and any irregular login attempts that may be deemed frivolous or a breach of this policy.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the Memorandum of understanding on Conduct of Service of 1994.
Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

11.7 COMMENCEMENT AND REVISIONS

This policy takes effect from the date determined by council in the resolution for its adoption, and will be reviewed annually or as the need arises, whichever comes first.

The policy may be amended from time to time as the need arises. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on the Municipality Website or Intranet, or by way of e-mail or memorandum.

12. IT DATA BACKUP POLICY

12.1 INTRODUCTION

Computer information systems and electronic data are valuable assets to Mopani District Municipality (MDM) and a substantial investment in human and financial resources has been made to create these systems, data, and information and, as such, a formalized policy has been developed, adopted and implemented to:

- Safeguard the information asset of the Mopani District Municipality;
- Prevent the loss of data in the case of accidental deletion or corruption of data;
- Permit timely restoration of information and business processes should such events occur
- Manage and secure backup and restoration processes and the media employed within these processes.

12.2 BACKGROUND

Municipality critical data and non-municipality critical data are stored on File-servers, Exchange-servers (mail-box data) and Application servers. This data can be categorized as:

- Personal User data (e.g. MS Word, Excel Spreadsheet, PowerPoint Presentations, etc.)
- Business Unit data (e.g. Reports, Plans. Etc.)
- Shared data (e.g. GIS, Maps, etc.)
- Databases (e.g. MS Exchange Email Server, GEMC3, etc.)
- Application / System data (e.g. ProMIS data, PayDay HR & Payroll, etc.)

All of the data listed above serve as records for Mopani District Municipality and must be safeguarded from all possible risks of loss.

12.3 PURPOSE OF THE POLICY

The purpose of this policy is to provide the Mopani District Municipality with a procedure for the change control function that shall be established to manage, record, and track all changes for Mopani District Municipality IT environment.

12.4 SCOPE OF THE POLICY

The scope of the policy covers those people who make use of MDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "USERS". Users are all permanent, contract and temporary personnel employed by the **MDM** who have been issued with a Municipality's Computer.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the Municipality's computers.

This policy is applicable to all servers on which data and system/application used by Mopani District Municipality resides. This includes servers that are either leased to Mopani District Municipality or brought onto Mopani District Municipality for purposes of performing a function for or rendering services to Mopani District Municipality by contractors or their employees for purposes of rendering services to Mopani District Municipality.

12.5 POLICY STATEMENT

12.5.1 Backup Policies

ITO will provide policy-based, system level, network-based backups of server systems under its stewardship.

Working with the **MDM** users, vendors for various application systems in production within **MDM**, and various directorates and various sub-directorates, **ITO** will implement backup policy on a per system basis that defines:

- **Selections**: what information is to be backed up on systems?
- **Priority**: relative importance of information for purposes of the ordering of backup jobs.
- **Type**: the frequency and amount of information to be backed up within a set of backup jobs.
- **Schedule**: the schedule to be used for backup jobs.
- **Duration**: the maximum execution tine a backup job may execute prior to its adversely affecting other processes.
- **Retention Period**: The time period for which backup images created during backup jobs are to be retained.

12.5.2 Definition of Retention Period

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed on **ITO**-maintained systems during the time period defined by system backup policies. Backup retention periods are in contrast to retention periods for information defined by legal or business requirements. System backups are not meant for the following purposes:

- To archive data for future reference.
- To maintain a versioned history of data.

12.5.3 Data to be Backed Up

All data residing on MDM servers will be backed up. This data includes the following:

(vii) Users data stored on the home directories ("My Documents") residing on File Servers through mapped home folder (network drive H :)

(viii) Shared data stored on file servers
(ix) System state of all servers
(x) Microsoft Exchange Server Information Stores (both Private & Public)
(xi) ProMIS (Financial Management System) data files
(xii) PayDay HR & Payroll data files
(xiii) SQL Databases (Web helpdesk, Symantec Endpoint Protection, etc.)
(xiv) Roaming User Profiles for all users logging on the network
(xv) Collaborator (Records Management System) data files
(xvi) General Emergency Management Command and Control Centre (GEMC3) data files
(xvii) ArcGIS GIS Maps and data
(xviii) Configuration data for Squid Proxy

12.5.4 Excluded Data Files

All multimedia files (e.g. photos, sound, music, videos, etc.) that are not associated to any system applications running on **MDM** server will be omitted during the backup process.

No data stored on the local disks or removable storage devices attached to workstations will be included in the backup. Only data residing on servers or networks storage will be backed up.

All files that are running or open during a backup routine will not be backed up due to technical limitation of the backup application in use at **MDM**.

On the home directory folders ("My Documents") stored on the network drive H: not all files will be backed up. The following are file extensions for files that will be omitted:

- .GIF
- .JPG
- .MPEG
- .MPG
- .MPA
- .MP2
- .MP3
- .MP4
- .EXE
- .VOB
- .WSF
- .WMA
- .WAV

12.5.5 Default Schedule of Backups

Unless a system supporting an application or business function requires a custom schedule, **ITO** will backup systems using a default schedule of weekly full backups and subsequent differential-incremental backups prior to the next full backup.
During backups, point-in-time images of information stored in active, permanent storage (e.g. hard disks) will be copied to magnetic tape or other media over a private network or virtual private network medium.

Full backups will back up all files specified within a system's backup policy, regardless of when they were last modified or backed up. Differential-incremental backups will back up all files that have changes since the last successful incremental or full-backup.

The media containing a system's weekly full backup and full set of subsequent differential-increment backups will comprise its weekly full backup media set.

Through use of weekly full backups and subsequent differential-incremental backups, backup windows (time period required to perform backups of one or more systems) will be minimized as will be the number of media required to store the backups. This will assist in ensuring good system performance for business processes.

Restores will require a longer period of time as the last full backup and all differential-incremental backups that have occurred since the last full backup are required. However, due to the frequency of backups, at most one week of tapes would be required in the event of a complete system failure.

Thus, this policy works to minimize the time required to backup systems (the common case) while limiting the potential time required to perform a full-system restore in the event of a system failure (the uncommon case).

ITO will schedule backup windows for systems so as to minimize disruption to business functions and ensure accomplishment of the weekly full – daily differential-incremental policies described above.

12.5.6 Storage Locations and Retention Period of Backups

Unless a system supporting an application or business function requires a custom retention period, **ITO** will maintain 12 weeks of full and incremental backups.

Backup tapes for the current weekly backup period will be stored within the Data Centre/Server Room for purposes of current backups and restores.

Tapes representing backups from the former weekly backup period will be maintained within a designated secured, fireproof safe within **MDM**'s offices until such time as the backup images stored on these tapes expire and the tapes are re-used or destroyed.

After a successful full weekly backup, a copy of the full backup's images will be made and stored in a secure, off-site media vaulting location for the period of one month for disaster recovery purposes. This will ensure that no more than one week of information would be lost in the event of a disaster in which **MDM** systems and backup images are destroyed.

After the period of a month has elapsed, the tapes will be returned to **ITO** and re-used or destroyed.

12.5.7 Backup Verification

On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:

- To check for and correct errors
- To monitor duration of the backup job
- To optimize backup performance where possible

ITO will identify problems and take corrective actions to reduce any risks associated with failed backups.

Test restores from backup tapes for each system will be performed at least every three months (quarterly). Problems will be identified and corrected. This will work to ensure that both the tapes and the backup procedures work properly.

ITO will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

12.5.8 Systems Management

ITO will ensure on an on-going basis that all elements of its backup system are documented and maintained in such a manner as to ensure:

- the integrity and confidentiality of data copied during backup and restore operations
- appropriate access to data maintained within the backup system
- recoverability in the face of system failure or disaster
- optimal performance
- stability

Elements of the backup system requiring on-going systems management include, but are not limited to:

- client software
- hardware drivers
- server software
- network connectivity and communications
- storage devices (e.g. tape library)

12.5.9 Media Management

Media will be clearly labelled and logs will be maintained identifying the location and content of backup media.

Backup images on assigned media will be tracked throughout the retention period defined for each image. When all images on the backup media have expired, the media will be re-incorporated amongst unassigned (available) media until re-used.

Periodically and according to the recommended lifetime defined for the backup media utilized, **ITO** will retire & dispose of media so as to avoid media failures.

12.5.10 Storage, Access, and Security

All backup media must be stored in a secure area that is accessible only to designated **ITO** staff or employees of the contracted secure off-site media vaulting vendor used by **ITO**.

Backup media will be stored in a physically secured, fireproof safe when not in use.
During transport or changes of media, media will not be left unattended.

12.5.11 Retirement and Disposal of Media

Prior to retirement and disposal, **ITO** will ensure the following:

- the media no longer contains active backup images or that any active backup images have been copied to other media;

- the media's current or former contents cannot be read or recovered by an unauthorized party;

With all backup media, **ITO** will ensure the physical destruction of the media prior to disposal.

12.5.12 Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration of information will be made through processes defined within **ITO**'s Procedure Manual or the prescribed Data Restore Request Form.

As the restoration of information has security consequences including:

- possible escalation of privileges by parties authorized to access information
- access by non-authorized parties

ITO will carefully verify that the request for restoration of information is authorized by the owners of the information prior to performing the restoration.

ITO will additionally ensure that the information restored is restored to a file system location with access controls appropriate to the information being restored.

12.5.13 Degradation of Service

Should a failure or defect of the backup system threaten the recoverability of a computing system or its information, **ITO** will take immediate actions to correct the situation.

Additionally, **ITO** will attempt to warn all users and owners of applications & information of the failure or defect and the potential scope of information loss.

ITO will work with those warned to mitigate potential or actual risks until such time as full-service can be restored.

12.5.14 Disaster Recovery Considerations

As soon as is practical and safe post-disaster, **ITO** will:

- Restore existing systems to working order or obtain comparable systems in support of defined business processes and application software.
- Restore the backup system according to documented configuration so as to restore server systems.
- Obtain all necessary backup media to restore server computing systems
- Restore server computing systems according to the priority of systems and processes as outlined for restoration and recovery by:
    - Mopani District Municipality Disaster Recovery Plan, or
    - Mopani District Municipality Business Continuity Plan, or

- The point-in-time direction of the Mopani District Municipality Senior Management or Mayoral Committee, and Council.

12.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "IT Change Management Policy". These duties include, but are not limited to Investigation of alleged or suspected non-compliance with the provisions of this policy.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the Memorandum of understanding on Conduct of Service of 1994.

Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

12.7 COMMENCEMENT AND REVISIONS

This policy takes effect from the date determined by council in the resolution for its adoption, and will be reviewed annually or as the need arises, whichever comes first.

The policy may be amended from time to time as the need arises. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on the municipality's website or intranet, or by way of e-mail or memorandum.

13. IT DISASTER RECOVERY POLICY

13.1 INTRODUCTION

This policy defines acceptable methods for disaster recovery planning, preparedness, management and mitigation of IT systems and services at Mopani District Municipality. The disaster recovery standards in this policy provide a systematic approach for safeguarding the vital technology and data managed by the Information Technologies Office. This policy provides a framework for the management, development, and implementation and maintenance of a disaster recovery program/plan for the systems and services managed by ITO.

This Policy forms the basis for the IT Disaster Recovery Plan and will link to the Mopani District Municipality's Business Continuity Planning.

13.2 BACKGROUND

Businesses, large and small, including government institutions, create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the municipality. The impact of data loss or corruption from hardware failure, human error, hacking, malware, or even from fire and natural disasters could be significant. A plan for data backup and restoration of electronic information is essential.

An information technology disaster recovery plan (IT DRP) should be developed in conjunction with the business continuity plan in order to guard against any unforeseen loss of this vital asset. Priorities and recovery time objectives for information technology should be developed during the business impact analysis. Technology recovery strategies should be developed to restore hardware, applications and data in time to meet the needs of the municipal business recovery.

13.3 PURPOSE OF THE POLICY

The purpose of this policy is to ensure that recovery strategies are developed for Information technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity. Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis. IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective for the business function or process that depends on the IT resource.

Information technology systems require hardware, software, data and connectivity. Without one component of the "system," the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)

- Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- Data and restoration

13.4 POLICY SCOPE

The scope of the policy covers those people who make use of MDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "USERS". Users are all permanent, contract and temporary personnel employed by the MDM who have been issued with a municipality's Computer.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the municipality's computers whenever applicable.

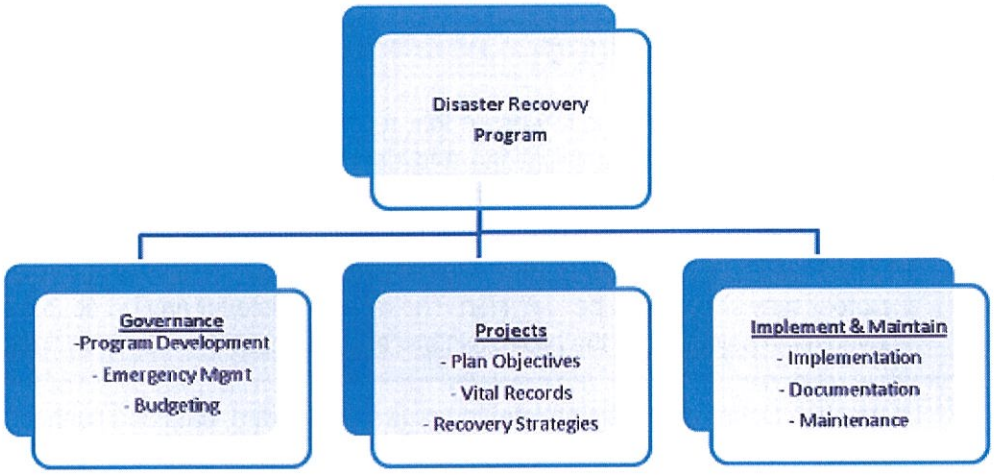
This policy is applicable to all servers on which data and systems/application used by Mopani District Municipality resides. This includes servers that are either leased to Mopani District Municipality or brought onto MDM for purposes of performing a function for or rendering services to MDM by contractors or their employees for purposes of rendering services to MDM.

13.5 POLICY STATEMENT

This policy defines acceptable methods for disaster recovery planning, preparedness, management and mitigation of IT systems and services at Mopani District Municipality.

13.5.1 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:



13.5.2 Governance

(i) All ITO-managed systems must comply with MDM disaster recovery policies and requirements.

(ii) The Assistant Director for IT, assisted by personnel in the ITO, ICT Steering Committee, and any duly appointed outsourced IT services provider, is responsible for IT Disaster Recovery (DR) program coordination and project management: including reporting status of IT DR planning, testing, and auditing activity to senior management committee on a regular basis; at least twice per year.

(iii) Senior management committee, assisted by the ICT Steering Committee, is responsible for ensuring sufficient financial, personnel and other resources are available as needed.

(iv) The Assistant Director for IT will review and update the DR Policy as necessary at least once per year. Any modifications on the DR Policy must be approved by the ICT Steering Committee, and it they necessitate changes to the IT environment, infrastructure, and computer systems, and /or networks, these changes to DR Policy must also be approved by the CMB.

(v) The Director for Corporate Services must ensure that all modifications to the DR Policy are approved by senior management committee and adopted by Council as required by law.

13.5.3 Program Development

(i) The IT Disaster Recovery Program (DRP) addresses the protection and recovery of MDM IT services so that critical operations and services are recovered in a timeframe that ensures the survivability of MDM and is commensurate with customer obligations, business necessities, industry practices, and regulatory requirements.

(ii) Plans must be developed, tested, and maintained to support the objectives of the Program stated in 13.5.3 (i), and those plans should include relevant IT infrastructure, computer systems, network elements, and applications. At minimum, annual updating is required.

(iii) The Assistant Director for IT is responsible (either in person or through delegation or duly appointed service provider) for conducting Business Impact Analyses (BIA) to identify the critical business processes, determine standard recovery timeframes, and establish the criticality ratings for each; at least once every two years.

(iv) The Assistant Director for IT is responsible (either in person or through delegation or duly appointed service provider) for conducting Capability Analyses (CA) to determine ITS's capacity to recover critical IT services that support defined critical business processes and recovery objectives; at least every other years.

(v) The Assistant Director for IT is responsible for maintaining the Recovery Tier Chart, which defines the Recovery Time Objectives (RTO) and Recovery Point Objectives

(RPO) of all ITO-managed systems. The Directors responsible for various business units are required to prioritize IT processes and associated assets within their directorates of responsibilities based upon the potential detrimental impacts to the defined critical business processes.

(vi) ITOS is required to create disaster recovery plans for the IT portion - including services, systems, and assets - of critical business processes. These IT services, systems, and assets must be inventoried and correlated according to the technical service catalog, prioritized based upon results of the Business Impact Analysis, and ranked according to their Recovery Time Objectives and Recovery Point Objectives.

(vii) A Risk Assessment must be conducted, at least once per year, to determine threats to disaster recovery and their likelihood of impacting the IT infrastructure.

(viii) For each risk or vulnerability identified in the Capability Review and Risk Assessment, a mitigation or preventive solution must be identified.

(ix) The IT DR program must include a change management and quality assurance process.

(x) The above Program Development statements will be progressively fulfilled via IT Office, Corporate Services Directorate, Office of the Municipal Manager, and/or all other resources at the disposal of the municipality.

13.5.4 Emergency Management

(i) The IT Disaster Recovery Team, along with the Assistant Director for IT is responsible for overseeing IT DR activities in the event of an emergency -i.e., an unplanned outage where RTO is in jeopardy.

(ii) The IT Disaster Recovery Manager should be part of the ITS representation within the institution's Emergency Management Team.

(iii) The ITO must develop and maintain a documented emergency plan including notification procedures.

(iv) Each Directorate shall account for its employees when a building evacuation is ordered. Supervisory personnel are responsible to account for the employees they supervise.

(v) The IT Disaster Recovery Team is required to complete a post-mortem report documenting outages and recovery responses within 60 days after the occurrence of a disaster recovery event.

13.5.5 Budgeting

(i) IT DR budgeting must be informed annually by requirements gathered in the BIA and CA as well as the ITO budgeting process.

(ii) ITO is responsible for tracking and reporting on planned and unplanned outage spending related to the recovery and restoration effort. During an outage, ITO may incur special recovery and restoration costs that are unbudgeted. For a small outage, these costs would be immaterial; but for a longer outage, these costs could be significant.

13.5.6 Plan Objective

(i) IT DRP must provide information on Business Impact Analysis, Data Backup, Recovery, Business Resumption, Administration, Organization Responsibilities, Emergency Response & Operations, Training and Awareness and Testing.

(ii) Plans must contain Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

(iii) Technological solutions for data availability, data protection, and application recovery must be considered by data gathered by the BIA and CA.

13.5.7 Vital Records

(i) ITO must maintain a single, comprehensive electronic inventory of all servers, network equipment, relevant configuration, and model information, and the applications they support. This inventory should be aligned with the service catalog and the technical service catalog.

(ii) All Backup data must be labelled and logged (as per MDM IT Data Backup Policy), and be available for use during an emergency within stated recovery time objectives. A documented (MDM IT Data Backup Policy) decision making process will be used to determine what subset of backup data will be additionally encrypted, and stored off-site in a secured location outside of the geographical area of the system they are backups of.

(iii) DR plans must be stored in a single, comprehensive database.

(iv) Where applicable, DR plans owners have to be able to access a copy of emergency and recovery plan(s) independent of ITO services and/or network.

(v) Upon completion or update, DR plans must be sent to the ICT Steering Committee and Senior Management Committee for review.

(vi) Plan information must be reviewed and updated as warranted by municipal business and/or information systems environment changes, at least annually.

13.5.8 DR Plan Attributes

(i) DR plans must address an outage that could potentially last for a period of up to six weeks.

(ii) DR plans must identify risk exposure and either accept the risk or propose mitigation solution(s).

(iii) Backup strategies must comply with predefined businesses continuity requirements, including defined recovery time and point objectives. Backup strategies must be reviewed annually.

(iv) Recovery strategies must meet recovery objectives defined in the DR tier chart.

(v) 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.

(vi) Recovery strategies must be implemented within a previously agreed upon period of time, generally not more than 180 days after management approval.

(vii) 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.

13.5.9 Maintenance

(i) Plans must contain current and accurate information.

(ii) Planning must be integrated into all phases of the IT system life cycle.

(iii) IT DR tests that demonstrate recoverability commensurate with documented IT DR plans must be conducted regularly; as well as when warranted by changes in the business and/or information systems environment.

(iv) Backup media supporting critical business processes must be tested bi-annually. Reviews are required within 60 days after a test to correct exposed deficiencies.

(v) Plan revisions must be completed within 60 days after a DR test is completed.

(vi) The following maintenance activities must be conducted annually:

a. Updating the documented DR plan

b. Reviewing the DR objectives and strategy

c. Updating the internal and external contacts lists

d. Conducting a simulation/desktop exercise

e. Conducting a telecommunication exercise

f. Conducting an application recovery test

g. Verifying the alternate site technology

h. Verifying the hardware platform requirements

i. Submitting the DR Status and Recoverability Report

j. ITO is responsible for briefing staff on their (staff) roles and responsibilities related to DR planning, including developing, updating, and testing plans.

13.6 APPLICATION OF THIS POLICY

The ITO is largely responsible for the implementation and enforcement of this "IT Disaster Recovery Policy". These duties include, but are not limited to investigation of alleged or suspected non-compliance with the provisions of this policy.

Action may be taken against any negligent disregard or infringe this policy. Disciplinary action will be applied in a progressive manner in line with applicable policies and procedures in cases of disciplinary measures.

13.7 COMMENCEMENT AND REVISION

This policy takes effect from the date determined by council in the resolution for its adoption, and will be reviewed annually or as the need arises, whichever comes first.

The policy may be amended from time to time as the need arises. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on the Municipality Website or Intranet, or by way of e-mail or memorandum.

14. ELECTRONIC MAIL POLICY

14.1 INTRODUCTION

Electronic mail is an efficient and timely communication tool that can be used to accomplish **MDM** functions and conduct the Municipality's business within its organization, with other governmental bodies, with private sector organizations, and with the public sector. E-mail can help the **MDM** improve the way it conducts business by providing a quick and cost-effective means to create, transmit, and respond to messages and documents electronically. Well-designed and properly managed e-mail systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. Daily tasks are accomplished more rapidly as individuals use e-mail services for sending and receiving texts as well as avoiding telephone expenses.

There are a number of characteristics that distinguish electronic mail from other sources, such as paper records, telephones and information stored on electronic media such as diskettes. Awareness of these characteristics should guide individual and Municipality use of electronic mail services.

14.2 BACKGROUND

The Internet resembles an alliance of public networks that employ a common set of protocols for the purpose of communicating information. The use of the Internet therefore offers a plethora of opportunities and benefits for Users to increase individual access to information resources relevant to official duties. However, the Internet is also subject to significant security problems as it provides potential access to a variety of information sources not relevant / related to official duties. Hence, not all resources on the Internet provide accurate, complete or updated information. Users are compelled to continuously evaluate the validity of information found on the Internet. It is therefore a general policy that Internet access and electronic mail services be conducted in a responsible, ethical and legitimate / lawful manner.

14.3 PURPOSE OF THE POLICY

The purpose of this policy is to establish guidelines, define users' roles and responsibilities as well as minimum requirements governing the acceptable use of the **MDM** electronic mail services. This policy specifically pertains to the use of World Wide Web on the Internet and receipt, storage and distribution of electronic mail. By establishing and maintaining compliance with this policy, risks and costs to the Municipality can be reduced while the valuable potential of this communication tool is realized. The objectives of this policy are to assure that:

- The use of electronic mail services provided by **MDM** is related to, or for the benefit of the **MDM.**
- The use of internet and e-mail services contribute to the accomplishment of officials duties
- Users understand that e-mail messages and documents are subject to the same laws, regulations, policies, and other requirements as information communicated in other written forms and formats
- Disruptions to **MDM** activities from inappropriate use of e-mail services provided by the Municipality are avoided
- Users are provided with guidelines describing their personal responsibilities regarding confidentiality, privacy, and acceptable use of Municipality-provided e-mail services as defined by this policy.
- Potential risk to sensitive systems and/or information is minimized to acceptable level.

14.4 POLICY SCOPE

The scope of the policy covers those people who make use of MDM Information Technology resources, equipment, network infrastructures or facilities, hereinafter referred to as "USERS". Users are all permanent, contract and temporary personnel employed by the **MDM** who have been issued with a Municipality's Computer.

This policy refers to "Users" as all computer users at the MDM, whether they are permanent, on contract or temporary employees supplied by service-providers to the Municipality.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose employees use the Municipality's computers.

14.5 POLICY STATEMENT

14.5.1 MDM Responsibilities

- **MDM** has the responsibility to ensure that electronic mail services provided by the Municipality are used for internal and external communications, which serve legitimate council functions and purposes.

- The Municipality must familiarize each user with what is considered appropriate use of e-mail services provided by the Municipality.

- Managerial authority over electronic mail services must be defined, and user-training programs provided which addresses e-mail usage and policies. Municipality "E-mail User Agreement" for electronic mail services, which stipulates compliance to this "Electronic Mail Policy", must be signed by each user if they are to retain or be provided with e-mail services. Failure to sign the E-mail User Agreement will result in denial of electronic mail privileges for the individual.

- Any significant problems encountered in using e-mail communications should be brought to the attention of the ITO and where appropriate, **MDM** management should be notified.

14.5.2 User's Responsibilities/Access

This policy is intended to illustrate the range of acceptable and unacceptable uses of the Municipality's electronic mail facilities. Questions about specific uses related to security issues not covered in this policy statement and reports of specific unacceptable uses should be directed to the ITO. Other questions about appropriate use should be directed to the user's supervisor/manager.

Users should be aware of potential electronic mail security problems before transmitting private or confidential messages. Electronic mail is not private communication. All information transmitted via the Municipality's Internet/e-mail system is the property of the Municipality and can be reviewed at any time. E-mail correspondence may best be regarded as a postcard rather than as a sealed letter. Disclosure may occur intentionally or inadvertently when an unauthorized user gains access to electronic messages. Likewise, disclosure may also occur when e-mail messages are forwarded to unauthorized users, directed to the wrong recipient, or printed in a common area where others can read them. Because of the various security, legal, and productivity issues referenced in this policy, each user has the following responsibilities:

- As an e-mail participant, each user must comply with this "Electronic Mail Policy" and the Municipality's "E-mail User Agreement" for e-mail services.
- Users must be aware of the classification of any information contained in data files or correspondence which they are transporting using e-mail communications and to not exchange confidential information in an un-encrypted form.
- Under no circumstances should data ever be transported, which if intercepted, would place the Municipality in violation of any law.
- The content of any information exchanged (sent or received) via electronic mail communications (regardless of its state of encryption) must be appropriate and consistent with Municipality policy, subject to the same restrictions as any other correspondence.
- Users granted access to electronic mail services need to use that access in a way which is consistent with their job function even when the access is outside working hours.
- E-mail communications, if allowed to accumulate on a server, can quickly consume the server's storage disk space and may cause system problems. Although deletion of unnecessary email communications is encouraged, users should consult the ITO regarding their record retention guidelines for proper instruction regarding disposal or archival of e-mail correspondence.
- Any Direct Connected Access to Internet and/or electronic mail services from official computers, networks and/or communication services must occur through accredited gateways or firewalls.
- No Remote (dial-in) Access is permissible due to security risks associated with dial in and out facilities.
- No remote or external connectivity will be allowed without prior knowledge of the ITO.

14.5.3 Principles of Acceptable Use

As with any Municipality-provided resource, the use of electronic mail services should be dedicated to legitimate Municipality business and is governed by rules of conduct similar to those applicable to the use of other information technology resources. Use of e-mail services is a privilege which imposes certain responsibilities and obligations on users and is subject to government policies and laws.

Acceptable use must be legal, ethical, reflect honesty, and show restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment and unwarranted annoyance.

All email users should:

- Comply with Municipality policies, procedures, and standards;
- Protect other users' privacy and confidentiality;
- Be responsible for the use of their email accounts;
- Use Information Technology resources efficiently and productively;
- Comply with all Municipality policies, controls, procedures, and standards
- Be courteous and follow accepted standards of good etiquette. Users must abide by the etiquette rules, not limited to the following:
    - ♥ Be polite;
    - ♥ Use appropriate language;
    - ♥ Refrain from revealing personal particulars about themselves and other users to anyone else on the internet or through email;
    - ♥ Refrain from revealing credit card details, credit checking accounts, or identity numbers on the internet or through email;

- ♥ Not attempting to gain illegal access to system programs or computer equipment;
- ♥ Use all appropriate precautionary measures to detect and if necessary prevent its spread through email or the internet;

14.5.4 Users Roles and Responsibilities

By signing the "Acknowledgement Letter", the User acknowledges that he/she has read the terms and conditions of this policy and understands its significance. Access to Municipality Internet and electronic mail services is a privilege, not a right. **MDM** networks, internet access and electronic mail services are to be used in a responsible, efficient and legitimate, and lawful manner and must be utilised to realise the objectives of the Municipality.

- Ensure that technical personnel from the ITO examine Internet traffic, electronic mail routing and information content in order to effect the legitimate performance of their official duties.
- Provide administrative assistance in the implementation of this policy.
- Understand and comply with the rules and conditions as set forth in the Policy.
- Not to add, delete or modify system files or change system setup on workstations made available to them.
- Not to log onto the Internet or use electronic mail using identification other than his or her own.
- Not allow any other person the use of his or her username and password to access the Internet and/or disseminate electronic mail from his or her official computer except when authorised to do so.
- To accept limitations or restrictions on computing resources such as storage space or amount of resources consumed.
- Not create access, display, download or transmit any text, image, or sound clip that include material which is obscene, libellous, or which advertises any product or service not permitted by law or that undermines the integrity and professional ethos of the municipality.
- Not to engage in any activities to damage hardware or software, disrupt communication services, waste system resources or overload networks with excessive data.
- Maintenance of Internet access and also the use of electronic mail services, content or otherwise, is constantly and vigilantly monitored and managed by the Information Technology Division to ensure quality and reliability of the systems. However, such monitoring may also be used to detect possible misuse thereof.

14.5.5 Privacy and Confidentiality

There can be no expectations of personal privacy or confidentiality in the use of Internet and electronic mail services since Internet access and electronic mail are subject to disclosure laws and record retention requirements

All information generated by the User through the use of the municipality Internet access and electronic mail services will remain the property of the municipality.

Internet and e-mail access and usage may be monitored by ITO to minimize and control abuse of these services.

14.5.6 Acceptable Activities

Acceptable e-mail activities are those that conform to the purpose, goals, and mission of MDM and to each user's job duties and responsibilities. The following list provides examples of acceptable uses:

Communications, including information exchange, for professional development or to maintain job knowledge or skills

Communications with other Municipality's agencies providing document delivery or transferring working documents/drafts for comment;

Announcements of Municipality procedures, hearings, policies, services, or activities;
Use involving research and information gathering support of advisory, standards, analysis, and professional development activities related to the user's duties;

Communications and information exchanges directly relating to the mission, charter, and work tasks of the Municipality including electronic mail in direct support of work-related functions or collaborative projects;

Limited personal use is allowed, subject to it conforming to this policy document and all other policies of **MDM**;

Communications, including information exchange, for professional development or to maintain job knowledge or skills.

NOTE:

- Users may be subject to limitations on their use of e-mail as determined by the appropriate supervising authority.

- Users are advised to remove themselves from electronic mailing lists not dealing with work-related topics.

- No User is allowed to attach the **Municipality letterhead with the Logo or Emblem**. No electronic signature containing the **MDM** details such as the letterhead should be attached to personal e-mail.

14.5.7 Unacceptable Activities

Unacceptable use can be defined generally as activities that do not conform to the purpose, goals, and mission of MDM and to each user's job duties and responsibilities. Any e-mail use in which acceptable in which acceptable use questionable should be avoided. In other words, when, in doubt seek policy clarification prior to pursuing the activity. The following list provides examples of unacceptable uses:

- Private or personal for-profit activities. This includes use of e-mail services for private purposes such as marketing or business transactions, private advertising of products or services, and any activity meant to foster personal gain;
- Unauthorized not-for-profit business activities. This includes the conducting of any non-governmental related fund raising or public relations activities such as solicitation for religious and political causes;
- Transmission of incendiary statements which might incite violence or describe or promote the use of weapons or devices associated with terrorist activities;
- Use for, or in support of, unlawful/prohibited activities as defined by Provincial and National laws or regulations.

Note: Unacceptable and forbidden User behaviour regarding access to Internet and e-mail services encompass, but are not limited to:

- Using profane, obscene, pornographic or other graphic pictures, which may be offensive and / or defamatory to others
- Using the Internet to search, access, store and retrieve information that is racist, violent, offensive, sexually explicit (sexually explicit content includes e.g. Cartoons, Text Messages as well as Photographs)
- No User shall engage in/respond to- activities such as political/religious statements, cursing and foul language as well as statements viewed as harassing or discriminative based on race, colour, creed, age, sex, physical handicap and/or sexual orientation
- Copying commercial software in violation of copyright laws
- Allow his or her User account and / or User password to be used by another person unless authorised to do so
- Distribute material for commercial purposes
- Engage in any activity that could compromise the security of the Municipality's host computer
- Electronic mailing to groups of people for unofficial purposes (as such, sending large volumes of unsolicited e-mail is prohibited.)

Note: Illegal activities relating to e-mail and network access include, but are not limited to:

- The transmission of threatening, offensive or harassing information (messages or images) which contains defamatory, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
- Violation of laws dealing with copyrighted materials (including articles and software) or materials protected by a trade secret;
- Intentionally seeking information about; obtaining copies of; or modifying contents of files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;

- The transmission of any information which encourages the use of controlled substances or uses the system for the purpose of criminal intent;
- Violation of Provincial and National laws or regulations prohibiting sexual harassment.
- Violating the privacy of individual users by reading their e-mail communications unless specifically authorized to do so;
- Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by the ITO. Assisting others in violating these rules by sharing information or passwords is also unacceptable behaviour;
- Deliberate interference or disruption of another user's work or system;
- The user must avoid any actions that cause interference to the network or cause interference with the work of others on the network. Users are prohibited from performing any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of system/network performance), or the introduction of computer worms or viruses by any means (use of programs with the potential of damaging or destroying programs and data);

  Distribution of "junk" mail, such as chain letters, advertisements, or unauthorized solicitations; and
- Unauthorized distribution of Municipality data and information.

14.5.8 Security Implications

The use of electronic mail services exposes the **MDM** and users to network and, in particular, Internet related risks. Even with the extensive effort that has been made by the **MDM** to minimize known risks, there is no known way to protect the Municipality from all related risks. E-mail and network security is a joint responsibility of SITA, Outsourced ISP Service Provider, DPLG, DLGH, ITO and e-mail users. Transmission of electronic mail to locations outside of the Municipality's local area network may require the use of the Internet for transport. Since the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls. Confidential and sensitive information must not be included in e-mail communications unless proper, formalized security precautions have been established. It is the responsibility of the ITO to protect confidential and sensitive information where intentional, inappropriate, or accidental disclosure of the information might expose the Municipality or an individual to loss or harm.

Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of their e-mail account by unauthorized individuals. Passwords should be changed with regular frequency or in accordance with the **MDM**'s policy regarding the frequency of changing passwords. Obvious passwords should be avoided. When users are away from their desks, precautions should be taken to protect their accounts (preferably shutting down the PC).

Much on Security has been covered in the Information Technology Security Policy.

14.5.9 Written Agreement Required

Users having access to electronic mail services provided by MDM are advised that all such network activities are the property on the Municipality, and therefore, they should not consider any activity to be private. All users of the e-mail services are required to acknowledge acceptance of and their intention to comply with this Electronic Email Policy by signing the Municipality's Information Technology User Declaration Agreement. Such signed agreements will be kept on the user's personnel file and copies thereof forwarded to the ITO.

14.6 APPLICATION OF THIS POLICY

The ITO is responsible for the implementation and enforcement of this "Electronic Mail Policy". These duties include, but are not limited to:

- Investigation of alleged or suspected non-compliance with the provisions of this policy; and
- Suspension of service to users, with or without notice, when deemed necessary for the operation and/or integrity of the Municipality's communications infrastructure, connected networks, or data.
- The ITO is able and reserves the right to monitor and/or log all network activity without notice, including all e-mail and Internet communications. Therefore, users should have no reasonable expectation of privacy in the use of these resources.
- While the **MDM** will not regularly monitor electronic- mail, users are on notice that the maintenance and operations of electronic message systems may result in observation of random messages. E-mail messages are not personal and private. E-mail system administrators will not routinely monitor individual staff member's e-mail and will take reasonable precautions to protect the privacy of e-mail.
- However, management and technical staff may access a user's e-mail:
    - ✓ for a legitimate business purpose (e.g. the need to access information when a user is absent for an extended period of time);
    - ✓ to diagnose and resolve technical problems involving system hardware, software or communications; and/or to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.
    - ✓ by participating in the use of networks and systems provided by the **MDM**, users agree to be subject to and abide by policies governing their usage. **MDM** management will review alleged violations of this policy on a case-by-case basis.

Some aspects of this policy are for information; others tell employees what they may and may not do. Action may be taken against users who disregard information or infringe this policy. Disciplinary action will be applied in a progressive manner in line with the applicable code of conduct for MDM employees, policies of the municipalities and labour laws of RSA.

14.7 COMMENCEMENT AND REVISIONS

This policy takes effect from the date determined by council in the resolution for its adoption, and will be reviewed annually or as the need arises, whichever comes first.

The policy may be amended from time to time as the need arises. Such amendments shall, as soon as reasonably possible, be brought to the attention of all users, including by posting such amendments on the Municipality Website or Intranet, or by way of e-mail or memorandum.

16. GUIDELINES ON THE USE OF IT AND OTHER COMPUTER EQUIPMENTS

16.1 PURPOSE

The purpose of this document is to regulate the use of all IT related systems, applications, and resources so that the Municipality can:

- Control costs with a standardized set of hardware and software that can be well supported and maintained;
- Use IT equipment economically and productively;
- Minimize risk of damage, loss, and theft of IT equipment.

16.2 WHO IS AFFECTED?

Every employee of the municipality, Councilors, temporary and contracted staff, consultants and their staff using MDM IT systems and applications will be affected by this guidelines and procedures.

This guidelines and procedures must also be applicable to all those IT service providers contracted to the municipality, whose personnel have access to MDM systems and applications.

16.3 PROCEDURE AND GUIDELINES STATEMENT

16.3.1 Allocation IT Equipment

Through a request from your manager, you may be issued with a computer and other IT related equipment or resources. All are provided to you to help you perform your duties effectively and efficiently so.

Allocations of computers to officials will be according to the Municipality's IT equipment standards document or guidelines as addressed in the IT Asset Management Policy, however if non-standardized equipment is required, then a recommendation should be made to the ITO. All equipment provided to users by ITO will remain the property of the Municipality and can be re-allocated to perform other tasks if need arises.

No procurement of computer-related equipment and software shall take place without an appropriate recommendation from the ITO.

16.3.1.1 Allocation of Portable Computers (Laptop/Tablets)

The use of personal computers and laptops has become an integral part of fulfilling an employee's daily task and responsibilities. To this end, the municipality provides employees with the access to personal computers or workstations to enable them to fulfill such duties and responsibilities.

In certain instances, the nature of an employee's job necessitates access to a notebook (portable personal computer) or handheld computer. This section serves to clarify the municipality's approach regarding MDM provided notebooks.
Management reserves the right to amend or provide exceptions to this document in specific instances. Below are the criteria that will be followed in allocation of portable computers:

- All employees on post levels 0 to 3 will be allocated a portable computer (laptop).

- Employees who require access to portable personal computers for the purpose of fulfilling their normal daily responsibilities will submit a motivation to the Information Technology Office through the head of the directorate where they report.

- Laptops remain the property of the municipality and must be returned on the employee leaving the employment of the municipality. The staff members are responsible for ensuring all appropriate steps are taken to avoid accidental damage to, loss or theft of the laptop allocated to them. All other employees who are required to use, or have access to computer systems, will only be given access to desktop personal computers or computer workstations.

- Any employee who has been allocated a portable computer will not be allocated a desktop computer, unless their job functions require that they have access to bother a portable and a desktop computer. Such deviations will require motivation by the concerned employee to the head of their directorate and approval by ITO.

16.3.1.2 Printers

- Printers will be allocated to officials depending on their specific needs.

- Desktop printers will be allocated to users who frequently print confidential official documents.

- Color printers will only be allocated on a needs basis to those staff members requiring such access to perform their duties.

- Specialized needs printing such as plotting/mapping and label printers will be acquired and allocated on needs basis after approval of motivation for such by ITO made through the head of the concerned directorate.

- General staff will be required to use shared LAN connected high speed laser printers nearest to them.

16.3.2 IT Equipment Standards

Acquisition of software and hardware must adhere to the municipality's standards to avoid user's personal preferences and determine the choice of hardware and software.

The standards document specification will be revised time to time, as and when the need arises. The standards document will cover the following areas:

- Specifications of the required desktop computer, including printers, notebooks, and other IT related equipment.
- The manufacturer or brand of the equipment.
- All standard software, systems, databases used in the district.

- Critical and non-standard software and other IT equipment.

If the Information Technology Office approves to raise the standard, all computers below the standard will be upgraded or replaced, without the need to motivate.

The goal is to obtain the best value for the product, better-negotiated service agreement and adequate support. It may also be required to purchase particular products from selected vendors/manufacturers because of the support and services offered (e.g. only XYZ desktop computer may be purchased due to extended warranty provided by XYZ). Though these will be centrally managed, all purchases should adhere to other numerous MDM policies, procedures and/or any other applicable regulations or acts of municipal government.

Analysis of hardware may include: -

- Appropriate software for the required task.
- System that comply with Technical Architecture or IT Strategy (Information security issues).
- Value for price, performance, reliability, adequate capacity and support issues due to unexpected failure of hardware.

Long term organizational business needs must be taken into account to avoid change of systems before their end of life as this may prove expensive for the municipality

16.3.3 New Positions and Appointments

When appointing a new employee for whom a computer is needed, and during resignation, Human Resources Unit must immediately notify Information Technology Office after the decision has been taken to fill or create the post. Such notice must be in writing accompanied by detailed job description of the incumbent. When current positions are being filled, the new appointee will be allocated with the computer that was allocated to the predecessor for as long as it is within its life cycle. If any changes/upgrades are required to meet the needs of the new employee, it will be responsibility of Information Technology Office to acquire the required hardware and/or software to meet these needs before the incumbent resumes his/her duty.

16.3.4 Computer and Software Maintenance

- Information Technology Office will maintain records of all hardware warranty and software upgrades agreements.

- All computer systems and its peripherals purchased through Information Technology Office should be covered by warranty and serviced by the vendor or agents appointed by the vendor during the warranty period.

- The cost of ordinary repairs outside of or beyond the period of warranty should be budgeted for and paid from appropriate ITO budget.

- Repairs to IT equipment should be done with economic value and use in mind.

- Information Technology Office will only perform software or hardware upgrades or maintenance on any equipment that has MDM asset tag attached. No

installation or maintenance of hardware or software will be performed on privately owned personal computers

- The Municipality retains the exclusive right to determine the hardware and software configuration of any personal computers purchased or funded by it, including any peripherals hardware such as modems, network accessories, printers, etc. and may in its sole discretion determine the price range and approved suppliers of laptops funded or purchased by or through the institution.

- No software may be installed on any computers owned by the municipality without first ensuring that the municipality has the necessary software licenses of such software. The installation of any additional software must be weighed against the anticipated benefit.

- However, management reserves the right to amend or provide exceptions to this procedures and standards in specific instances.

16.3.5 Major IT Projects

Cost related to infrastructure changes, renovations, or office moves (e.g. re-cabling or installation of additional network points) must be included in the projects and budgeted for appropriately. Major cabling projects should be budgeted for and handled in conjunction with municipality's procurement policy for large spending e.g. cabling of the new premises.

16.3.6 Personal Use

Personal use of computers and IT services is allowed subject to the following conditions:

- Personal use should not affect service delivery.
- Personal use should not cause the municipality to incur direct or indirect costs.
- Personal use must comply with the content of the MDM IT Policies, Procedures and standards, and all other policies and applicable in the municipality.

16.3.7 User's Responsibility

Users will be expected to take care of the equipment issued to them. This is particularly more relevant to staff who use portable equipment such as Notebooks.

If the user loose or damage equipment or software that belongs to the Municipality it must be reported to Head of Directorate, and the Information Technology Office. *In case of theft or suspected theft, users must also report it to South African Police Services. This provision does not however supersede procedures set out in MDM Asset Management Policy and all other applicable policies and laws.*

Users may have to pay for lost, damaged or stolen portable computers or equipment if

- They have acted negligently.
- Intentionally caused the damage.
- Ignored any precautionary instructions given (such municipality circulars and memorandums).

In case the user requires municipality's computer outside the premises, either to work at home or at another remote office/site/building, the user must obtain written permission or authorization from the head of directorate and BTO unit responsible for asset management, and approval from ITO, before the equipment is removed. The permit must indicate your name as well as the description of the equipment to be removed, the date of removal and return.

16.3.8 Inappropriate Material

Users are not allowed to store information or material that can be considered offensive; this includes words, images or recorded sounds.

Users must not store files that have any form of the following information, political opinions, pornography, violence, nudity, racisms, sexism, xenophobia, etc., or that which has the potential to incite violence, labour unrest, or bad working environment.

In case the above have been stored on a computer by another user, either accidentally or in violation of the policies, procedures and/or standards, the municipality will not be held responsible for such material, either viewed intentionally or unintentionally. ***If users discover this kind of offensive material in their computers, or that of other users, such material must be reported to the ITO.***

16.3.9 Managers' Responsibility

- Directors/Managers have the right to monitor the use of computer systems and applications by officials within their directorates/departments/units.

- Directors/Managers must ensure that all staff within their directorate/units using computer systems and applications, permanent, temporary or contracted, including contracted service providers and their staff using MDMD computers systems, application and networks are made aware of this policy. The Directors/Managers are required to apply this policies/procedures and standards to all those who report within their directorate/units.

16.3.10 Grant Funding

A directorate/department preparing a proposal for funding involving computer hardware, software, and applications should consult Information Technology Office. ITO will assist in identifying hardware/software that is supported and will work best on the MDM information technology infrastructure.

16.3.11 DON'T's and DO'S

You are not allowed to

- Bring your home computer along to the office.
- Move your computer without informing the ITO, head of directorate and BTO asset management unit.
- Put your coffee/tea cup on top or close to your computer.
- Disconnect your PC for a reason not known to the ITO.
- Install a third party software or non-standard software, unless authorized to do so.
- Install computer games or other entertainment software.

- Repair or perform any form of upgrade to the computer equipment.
- Swap computer equipment with other users.

You must

- Switch off your computer at the end of each working day and over weekends, unless authorized and instructed otherwise by the ITO.
- Be logged into the network when using MDM computer whenever in the office.
- Obtain a permit before taking an equipment offsite, unless it is a notebook officially allocated to you.
- Always keep your desktop computer tidy.
- Inform Information Technology Office if you suspect malfunctioning of computer systems, equipment, or applications before it is too late.
- Report any unlicensed or suspected non-standardized software to the Information Technology Office.
- Clean your computer keyboard, mouse, system unit and monitor using cloth and/or chemicals approved and/or supplied by ITO.

16.3.12 Application of the Guidelines and Procedures

The procedures will be applied in different ways including:

- Where technology allows, this will be enforced using system-level group policies, e.g. people will be prevented from running executable files, automatic lock of critical areas of your desktop, etc.
- Information Technology Office monthly reports will highlight possible violations. The offender's director/manager will take disciplinary action in line with MDM disciplinary codes.
- Users will be expected to report any violation and/or deviations.
- The Information Technology Office may issue instructions via Corporate Services Directorate.

16.3.13 Disciplinary Action

Users may be subjected to disciplinary measures if they violate these guidelines and procedures, and it will be in line with the MDM disciplinary codes.

17. PROCEDURE MANUALS

17.1 PROBLEM MANAGEMENT

- Logging IT / IT Related Calls
- Please note that all end-users are expected to try and diagnose IT problems encountered before calling the IT Office.
  The following shall be checkpoint for users before a call is logged (in the order they appear): -
- All cable Connections
- All peripheral connections
- Power connections
- Reboot if possible (Switch off the plug on the wall socket)

17.2 CALL LOGGING PROCEDURES

Users call log on procedures

- User determines problem.
- Phone the IT Office.
- Explain the problem.
- IT Office offer first line support. (If problem solved is closed, if not escalated to Technician)
- Receive the reference number and name of technician.
- Technician liaise with the user, solve the problem, if not liaise with other team members, if not log with service providers.
- IT Office makes a follow up call (if necessary).
- Close the call (IT Office).

The turnaround time for IT service delivery is specified in 5-20 minutes depending on the location. The IT staff and the IT Office shall be measured as such.

17.3 Symantec Endpoint Protection Manager Procedures

17.3.1 How Live Update Works

Symantec LiveUpdate is a "pull" technology, which means that data is not directly sent to Symantec LiveUpdate servers. Instead, LiveUpdate examines your computer to create a list of the currently installed products, and then uses this list to make requests for updates to those installed products. In making requests for updates, the LiveUpdate server creates a server log entry that lists the files that were requested and the IP address from which the request came. If the requested file exists on the LiveUpdate server, it is downloaded from the server by the LiveUpdate client (in case of MDM the clients is the Symantec Endpoint Protection Manager Server) and the server log entry reflects that a successful download occurred. The server log also reflects if the file was not downloaded or if an error occurred during the download of the file. In addition to the name of the file that is being requested, LiveUpdate also includes some identifier information and some computer-specific information in its communication with the server as further described below.

17.3.2 About Data to be collected

LiveUpdate collects general system information from the SEPM each time LiveUpdate runs, so that the updates that works best with SEPM at MDMD are received. The information is also used to generate aggregate statistics about how LiveUpdate is used and which systems need support, so that the LiveUpdate client software and the content and patches made available via LiveUpdate can be improved.

This information includes the following:

- Product name and version information for any installed Symantec software that is requesting updates
- Server make and model
- Version information for the operating system and browser
- Region and language setting
- Globally Unique LiveUpdate Identifier (LU ID) and current session identifier
- LiveUpdate client version and information about how the LiveUpdate session was started
- Patch file name and error code for any updates that failed to download or install correctly

The MDM Internet Protocol (IP) address is logged when connection is made to a Symantec LiveUpdate server, but it is only used to generate aggregate statistics and is then discarded.

17.3.3 How collected data is used

To generate accurate statistics, LiveUpdate creates a globally unique identifier that is stored on the server to uniquely identify it (LU ID). The LU ID is created at installation by requesting a Globally Unique Identifier (GUID) from the operating system and then running that GUID through an SHA-1 algorithm to create the LU ID. This method ensures that the LU ID does not contain any information that can be used to identify you.

The LU ID can then be used in the following scenarios:

To provide quality control feedback to Symantec development teams, the number of individual computers that visit the LiveUpdate servers and whether the download and installation of specific updates succeeded or failed is recorded. The LU ID of the computer that attempted the download, the product names that updates were requested for, whether updates were required, and the configuration information listed are recorded.

Symantec also collects information about how often each computer runs LiveUpdate and the environments in which customers typically run LiveUpdate.

Any information stored by Symantec LiveUpdate is maintained in electronically secured database files at physically secure data centers located in the United States, and does not contain any personally identifiable information. Symantec does not aggregate the information stored by LiveUpdate with any data, contact lists, or subscription information that is collected by Symantec for promotional purposes.

17.3.4 Updating Definitions for the SEPM using a .jdb File

To download the .jdb certified definitions:

(i) In a browser, go to the "Symantec Endpoint Protection / Symantec Antivirus Corporate Edition" website at the following URL: http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=savce

(ii) There is multiple headings/product categories presented. Be aware that there is only one .jdb in the list that will need to be downloaded. This is sufficient in updating both 32 and 64 bit definitions on the SEPM.

To download the .jdb Rapid Release definitions:

(iii) In a browser, go to the "Rapid Release Virus Definitions" website at the following URL: http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=rr

(iv) Download the available .jdb file and save the file to the Windows desktop.

To use the .jdb file to update definitions for SEPM:

(v) After downloading, you may need to rename the file extension from ".zip" to ".jdb". (Most browsers detect the file type and automatically change the extension. This must be changed back to .jdb for use in the SEPM.)

(vi) Copy the .jdb file to "C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\inbox\content\incoming" for 32 bit operating systems and to "C:\Program Files(x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\content\incoming" for 64 bit operating systems. The location listed in this line is the default installation location and is presented as an example only.

(vii) Copy the .jdb file to "C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\inbox\content\incoming" for 32 bit operating systems and to "C:\Program Files(x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\content\incoming" for 64 bit operating systems. The location listed in this line is the default installation location and is presented as an example only.

(viii) The .jdb file will be processed, usually within one minute. As the .jdb file is processed, all files and subfolders are removed from the "Incoming" folder.

Verify that the SEPM content is updated:

(ix) To verify that the SEPM content has been updated, look in the following folders

a. For SEP 12.1 - Check for the following locations:

32 bit Definitions: "C:\Program Files\Symantec\Symantec Endpoint Protection Manager\Inepter\content\{535CB6A4-441F-4e8a-AB97-804CD859100E}"

64 bit Definitions: "C:\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\content\{07B590B3-9282-482f-BBAA-6D515D3855E2}"

b. Typically, there will be three or more numbered folders present. The folder naming convention is "yymmddxxx". For example "100602034". These are the date and build (revision) number of the definition set installed. Please note that the definition set installed may have been published the previous day and a set for the current day may not yet be available.

c. Looking inside the folder that matches the set downloaded and installed, there should be a folder named "Full" and a zip file named "Full.zip".

d. Looking inside the "Full" folder, there should be the files typically associated with a virus definition set.

17.3.5 Important Notes:

1. The Intelligent Updater file names for Symantec AntiVirus (SAV) clients end with "i32.exe" or "i64.exe" (32 and 64 bit respectively).

2. The Intelligent Updater file names for SEP clients end with "v5i32.exe" or "v5i64.exe" (32 and 64 bit respectively).

3. The Intelligent Updater file name that ends in "x86.exe" is only for specifically listed products and should only be used with those products.

4. The SEPM updater file has a ".jdb" extension. There should only be one .jdb listed at any time and will update content for both 32 and 64 bit systems.

5. The SAV Parent Server updater file has a ".xdb" extension and only updates 32-bit virus definitions; SAV parent servers do not serve 64 bit definitions. 64 bit systems cannot be SAV parent servers.

17.4 *End-User Procedures*

17.4.1 Network & PC Storage

All municipality-related data files shall be saved in the network folders –"Home directories or other designated folders".

17.4.1.1 Saving Files (First time only)

The MDM Information Technology system has been standardized to Microsoft® Windows® 10 Professional 64-bit and Microsoft® Office 2019 or Office365 Standard across the organization. In cases

All Microsoft Windows applications (used in the MDM) follow a similar procedure for saving files.

In the application (e.g. MS Word, Excel, Power point, Access, Projects, etc.):

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

17.4.1.2 Resaving files
(i) Click "file ","Save"
(ii) Click the "Save" button in the standard menu bar or
(iii) Alternative replace step (i) with Ctrl-S within the Microsoft® application.

17.4.1.3 Resaving Files (with a different name)
(i) Click "File",
(ii) Click "Save As"
(iii) Click the "Save AS " message box, change the file name
(iv) Click the "Save Button"

17.4.1.4 Open Saved File
(i) Click File,
(ii) Click Open,
(iii) Select the Saved File, and
(iv) Double Click the File.
(v) Alternatively replace step (i) and (ii) with Ctrl-O

17.4.1.5 Print
(i) Click File
(ii) Click Print
(iii) Alternative replace step (i) with Ctrl-P

17.4.1.6 Deleting Files
Deleting network files is permanent. Take care to ensure that you really want to delete these files. Restoring such files will require procedure set out in the Data Backup Policy. Deleting of PC files places them in the recycle bin.
(i) Double-click the "My Computer" button
(ii) Navigate to the folder where the file to be deleted is located,
(iii) Click the file once only (it will be highlighted / selected),
(iv) Press the "Delete " button on the keyboard,
(v) Confirm deletion by clicking the "Yes" in the confirmation window.

NB: A number of files can be selected at the same time by keeping the "Ctrl" button depressed and selecting various file one by one using mouse click, or by selecting various files that follow in sequence by depressing "shift on the" keyboard and using arrow keys to select files.

NB: Business files are to be saved in the network for security and backup purposes.

17.4.2 Handling E-mails

17.4.2.1. Creating new Mail

Inside the e-mail application "Outlook"

(i) Click the "New" icon-a blank window for new mail will appear,
(ii) Enter the correct destination e-mail address,
(iii) Enter the correct Heading / Subject for your correspondence,
(iv) Attach a file in necessary (see point to below on how)
(v) Click the "send" button.

17.4.2.2. Deleting Mail

Deleting mail is the same as deleting file in windows

(i) Inside the e-mail application "Outlook
(ii) Click the folder on the right hand column
(iii) Right click the mail item to be deleted
(iv) Select Delete or
(v) Alternatively –select the mail item and press the delete button

17.4.2.3 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

(i) Make sure that the cursor is at the right location
(ii) Click the "Attach File" icon on the menu ribbon. A dialog box "Insert File" will appear
(iii) Navigate to correct location and click file to be attached.
(iv) Click the Insert button. This will take you back to Outlook with the file attached.
(v) 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;

(i) Click File
(ii) Clicks Send To
(iii) Click Mail Recipient (As Attachment)

A new e- mail 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:

(i) Navigate to the folder that contains the file (s) to be attached,
(ii) Right click the files and select send to
(iii) Click mail recipient

A new e-mail message with the attachments will be open

Just fill in the other fields, type message, and proceed as usual.

17.4.2.4. 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.

(i) In Outlook, with the email windows open, double click the attached file to pen it.
(ii) If the attached file has no default application associated with it installed, a user may be require to select appropriate application/program to use to open the attachment.
(iii) 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
(iv)

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

17.4.2.5. 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.

(i) Right click the folder in which you want to create a sub-folder,
(ii) Click on "New Folder",
(iii) Enter the appropriate name for the folder to be created,
(iv) Click the "OK" button,
(v) The folder will appear back in Outlook.

17.4.2.6. 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: -
(i) Note the folder marked 'Personal Folders' and all its contents,
(ii) Select the mail files(s) to be moved from the right hand column,
(iii) 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
(iv) Personal "Folders" Selected items will be moved

17.4.2.7 Deleting Mail

(i) Make sure that a correct folder is selected e.g. Deleted Items or Inbox
(ii) Select the file to be deleted on the right hand column and press delete key on the keyboard.
(iii) 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 "",

(iv) 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.

17.4.2.8 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.

18. APPROVALS & ADOPTION

Resolution NO: SCD/16/2024	Approved Date: 16 May 2024
Effective Date:01 July 2024	Review Date: ANNUALLY

15.AUTHORITY

MUNICIPAL MANAGER
Mr T.J MOGANO

COUNCIL SPEAKER
CLLR N.M MASWANGANYI

ANNEXURE A - Minimum IT Equipment Specifications

Desktop Computer		Laptop Computer	Software installed
CPU	InteliCore i5	Intel Core i5	Application Software (***Windows 10 Professinal***)
RAM	4Gb (Dual Channel)	8Gb (Dual Channel)	Document Management System (***Collaborator***)
			Geographic Information System (***GIS***)
HDD	500Gb	350GB	Symantec End-Point Protection
Display Monitor	19inch LCD	10inch Integrated LCD	Operating System (***Ms Windows 10 Professional***)
			Finance Management System (***ProMIS***)
			HR and Payroll System (***PayDayWin***)
			Project Management Software

ANNEXURE B – Declaration Form

DECLARATION

I, the undersigned, acknowledge that I am an employee of Mopani District Municipality, and hereby declare:

1. CONTACT PARTICULARS

Title		**Initials**		**Surname**	

Employee No.		**Tel/Ext No.**		**Cellphone No.**	

Directorate		**Division**	

Office Number and Building (e.g. Old Parliamentary Building, office 52)	

2. The **Municipality,** through the ITO, is the rightful owner of the following computer equipment which has been issued to me, as listed hereunder, and for which I am responsible as a **User** with the following **User ID/Name:** .....
(Used to logon to **MDM** network/computer)

Asset Category	**Make**	**Model**	**Serial Number**	**Asset Number**
CPU / Desktop				
Display Monitor				
Printer ***(Complete if applicable)***				
Scanner ***(Complete if applicable)***				
Notebook/Laptop ***(Complete if applicable)***				

Other equipment *(Mark with an X)*	**Keyboard**	**Yes**	**No**	**Mouse**	**Yes**	**No**	**Speakers**	**Yes**	**No**

Additional Software		

3. As a registered User I am aware of, and undertake:

(a) To take reasonable care to prevent the wilful or negligent loss of or damage to the equipment;
The following factors should also be considered:
- In the event of damage to the equipment at any time while it is in the **user's** possession, the **user** agrees to inform the **ITO** immediately.
- The **User** agrees to pay the cost of repairs of all damage to the **equipment** caused by the **user's** lack of due care, negligence, or misuse.

(b) To make use of the Municipality support services of the ITO for the maintenance of the **equipment**;

(c) To adhere to all the Municipality IT Asset and Inventory Control Procedures, the municipality's IT Security policies and measures in this regard, as well as the BTO, SCM, National and Provincial Treasuries circulars and directives pertaining to the loss of or wilful damage to equipment;

(d) To notify the ITO as per **IT ASSET RELEASE FORM (ITRAF)** of my intention to move the **equipment** should it become necessary for the performance of my duties?

(e) To notify the HR and ITO in writing of my resignation and to return all of the **equipment** listed in terms of this Declaration to the ITO.

The following factor should also be considered:
- Failure of the **user** to return the **equipment** may result in the **MDM** taking legal action to recover said **equipment** and recover any damage thereto, or recover the depreciated value thereof, at their sole discretion.

4. With reference to the Support, Maintenance and IT Asset Control policies and the procedures and standards of **equipment** of the **Municipality**, the **User** also accepts:
(a) That all **equipment** will be configured and maintained by the **Municipality** only.
(b) That **equipment** may not to be exchanged between **Users** or workstations.

Signed at ..... on ..... day of ..... 20.....

.....

Signed (**USER**)

INITIALS: ..... SURNAME: ..... POSITION: .....

Signed (**ITO**): ..... Date: .....

WITNESS (User's Manager)

INITIALS: ..... SURNAME: ..... POSITION: .....

DATE: .....

FOR USE BY ITO

The Asset Register has been updated. YES NO

Name: ..... Signature: ..... Date: .....

ANNEXURE 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 occurs between locations and between users, and during the resignation of personnel]

FROM		TO	
1. Employee (user) [e.g. Mr. Mangena S)		**2. Employee (user)** [e.g. Mr Mangena S]	
3. Office & Building[e.g. Old parliamentary Building]		**4. Office & Building** [e.g. Old Parliamentary Building]	
5.Telephone Number		**6. Telephone Number**	
7. Division & Directorate [e.g. B&T]		**8. Division & Directorate** [e.g. B&T]	

Category (e.g. CPU)	**Make** (e.g. Mecer)	**Model** (e.g., Premium X)	**Serial no** (By manufacturer)	**MDM 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 form to the ITO

FOR USE BY ITO ONLY

The Asset Register has been updated. YES NO

Date .....

Name in print .....

Signature .....

ANNEXURE D – PASSWORD RESET REQUEST FORM

User Information

Surname: ..... Initials: .....

Network Username/ID: .....

Employee Number: ..... ID Number: .....

Directorate: ..... Unit: .....

Contact\Tel\Ext Number: .....

Reason for Password Reset

Password Forgotten ☐
Password Expired ☐
Suspected Breach/Disclosure (Provide Details) ☐

More Details

.....

.....

.....

.....

Acknowledgement and Authorization

I hereby request ITO 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 User Account and Password Management Policy and Password Policy.

Name.....

Signature..... Date..... Time.....

---------- **For ITO Use Only**----------

Password Reset By.....

System/Application/Resource.....

Signature: ..... Date: ..... Time.....

ANNEXURE E - INTERNET ACCEPTABLE USE UNDERTAKING (IAUU)

User Information

Surname and initials: .....

First Name: .....

Position: .....

Employee number: ..... ID Number: .....

Department: .....

Division: .....

Office: .....

Acknowledgement

I hereby acknowledge that I have read and understand all the contents of the Internet Acceptable Use Policy and agree to abide by all its provisions. I shall use Mopani District Municipality internet facilities in an acceptable manner as stated in the Internet Acceptable Use Policy. I understand that violation of this policy and all other policies that govern the use of Information Technology in Mopani District Municipality may result in disciplinary action, including possible termination and civil and criminal penalties. When in doubt of what constitutes violation, I shall take the full responsibilities of getting clarity and advice from my manager/supervisor or Information Technology Office.

User (Name): .....

Signature: ..... Date: .....

Witness/Manager (Name): .....

Signature..... Date.....

ITO (Name): .....

Signature: ..... Date: .....

ANNEXTURE F – PASSWORD RESET REQUEST FORM

User Information

Surname: ..... Initials: .....

Network Username/ID: .....

Employee Number: ..... ID Number: .....

Directorate: ..... Division: .....

Contact\Tel/Ext Number: .....

Reason for Password Reset

Password Forgotten ☐
Password Expired ☐
Suspected Breach/Disclosure (Provide Details) ☐

More Details

.....

.....

.....

.....

Acknowledgement and Authorization

I hereby request ITO 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 User Account and Password Management Policy and Password Policy.

Name.....

Signature..... Date..... Time.....

---------- **For ITO Use Only**----------

Password Reset By.....

System/Application/Resource.....

Signature: ..... Date: ..... Time.....

ANNEXTURE G – IT CHANGE REQUEST FORM

Service Request No.:	
Change Proposal Title:	Date:
Originator:	Directorate:

Description of Proposed Change: Implementation Date: Implementation Time:

Benefit of the Proposed Change to the user(s)/department/directorate/institution:

System/Server Name(s):		Change Type:	Hardware	Outage Required?	Yes ☐ No ☐	If yes, anticipated duration:	HH:MM

Impact/Risk Analysis Summary (Include the impact of not doing the change as well as identifying risks associated with this change)

Alternatives

Initial Review: By: ☐ Date: ☐ Approved? Yes ☐ No ☐ Addition Information/ Follow-up Required ☐
Reason:

IT CHANGE REQUEST FORM

Impact Analysis Detail Section: Classification: High ☐ Medium ☐ Low ☐
Directorate/Department Affected: Systems/Configuration Item(s) Affected: Cost Impact: Resources Impact:

Implementation Procedures/Schedule:

Testing Summary:
Test Plan
Testing Completed? Yes ☐ No ☐ Test Results:

Fall Back Plan:
Fall Back Procedures: What is the impact on user(s)/department/directorate/institution if a fall back plan is necessary?

Communication Plan:		
Notifications	Date	Notification Method Email ☐ Phone ☐ Meeting ☐ Memo ☐ Other ☐
		Email ☐ Phone ☐ Meeting ☐ Memo ☐ Other ☐
		Email ☐ Phone ☐ Meeting ☐ Memo ☐ Other ☐
		Email ☐ Phone ☐ Meeting ☐ Memo ☐ Other ☐
Was feedback provided by the user(s) regarding the change, impact, impact, scheduling, etc.?		

IT CHANGE REQUEST FORM

Change Management Board (IT Steering Committee):		
Review Date:		
Name:	Position/Dept.:	Signature:

Classification: High ☐ Medium ☐ Low ☐

Approved ☐
Date Scheduled:
Denied ☐
Reason(s):

Post Implementation Review:

Date of Post Implementation Review: _____ Was the change successful? Yes ☐ No ☐

Acceptance Testing Results:

Describe whether the goals of the change were met:

Was the change implemented:
On time? Yes ☐ No ☐

Within budget? Yes ☐ No ☐

Identify lessons learned:

Was the fall back plan executed? Yes ☐ No ☐
Describe the situation that precipitated the use of the fall back plan:

ANNEXURE H – FIREWALL EXCEPTIONS APPLICATION FORM

This form is used to apply for exceptions from the standard firewall TCP-IP ports, authentication, or the applications of this policy.

12.1 Procedure

Complete the following steps:

1. Read the Firewall Policy.
2. Complete the required information below
3. Sign and date in the spaces provided
4. Return a copy of this signed document to the **ITO**.

Source IP Address	
Source Contact	Name:
	Tel :
	Email:
Destination IP Address	
Destination	Protocol:
	Port :
Destination Contact	Name:
	Tel :
	Email:
Reason for requested exception	

12.2 Signatures

Your signature attests that you agree to the following terms:

I. I have received and read a copy of the Firewall Policy and all other relevant policies and understand and agree to same;
II. I understand that violations of the Firewall Policy and all other applicable policies could result in termination of my employment and legal action against me;

Employee Name: ..... Supervisor Name: .....

Employee No.: ..... Supervisor Employee No.: .....

Employee Directorate: ..... Supervisor Directorate: .....

Employee signature: ..... Supervisor Signature: .....

Date: ..... Date: .....

APPENDIX I – DATA RESTORE REQUEST FORM

User information

Surname and initials: .....First name: .....

Employee number: .....Department: .....

Office number: ....Telephone/Extension: .....

Address: .....City/Town: .....

Contractors must provide their birth date in this format to substitute the Employee no.: DDMMYYYY

I am requesting the following files or documents to be restored:

File name	Date Created	Update date	Deleted Date & time

Conditions:

All officials and contractors using the Departmental network and resources are subjected to Policies, Procedures and Standards as defined by Information Technology Services. Forms have to be submitted to IT Helpdesk for restoration.

Applicant signature: .....Date: .....

For ITO Use Only

Employee number and other information verified ( )

Name: ..... Signature: ..... Date: .....

APPENDIX J – BACKUP TAPE REGISTER

DATE	BACKUP DESCRIPTION	TAPE DESCRIPTION

APPENDIX K – BACKUP TAPES OUT-STORAGE REGISTER

DATE	NAME	TAPE IN DESCRIPTION	TAPE OUT DESCRIPTION	SIGNATURE

APPENDIX L – DATA BACKUP LOG

Week Beginning	Day	Drive Cleaned (Yes/No)	Tape Inserted by (Name)	Date	Tape No.	Tape Removed by (Name)	Date	Location of tape	Backup Status (Complete / Failed)	Action Taken Where Backup Failed
	Monday									
	Tuesday									
	Wednesday									
	Thursday									
	Friday									
	Monday									
	Tuesday									
	Wednesday									
	Thursday									
	Friday									

APPENDIX M – BACKUP PROCEDURE

Data backup name	Type of backup	Scheduling of backup	Time backup starts	Overwrite/append period	Media set name	Barcode number on tape	Backup strategy
Exchange Information Store Server: **MOPDC**	Working set		2300				Grandfather Father Son
	Differential	Every Monday	2300	1 week	MOPDC Monday		
	Differential	Every Tuesday	2300	1 week	MOPDC Tuesday		
	Differential	Every Wednesday	2300	1 week	MOPDC Wednesday		
	Differential	Every Thursday	2300	1 week	MOPDC Thursday		
	Weekly full	Every Friday	2100	3 weeks	MOPDC Friday		
	Monthly full	Every last day of the month	2300	1 Year	MOPDC Monthly		
Mailboxes Server: **MOPDC**	Full	Every 2nd Sunday			MB MOPDC		Full backup
System state Server: **MOPDC**	Full	Every 2nd Saturday			SS MOPDC		Backed up to a file. >File selection of backups for various additional server backups are then backed up to tape every 2nd week
User Home Folders Server: **SERVER-ADMIN**	Working set			Never/infinite			Grandfather Father Son
	Differential	Every Monday		1 Week/Infinite	SVR-ADMIN Monday		
	Differential	Every Tuesday		1 Week/Infinite	SVR-ADMIN Tuesday		
	Differential	Every Wednesday		1 Week/Infinite	SVR-ADMIN Wednesday		
	Differential	Every Thursday		1 Week/Infinite	SVR-ADMIN Thursday		
	Weekly full	Every Friday		3 Week/Infinite	SVR-ADMIN Fridays		
	Monthly full	Every last day of the month		1Year/Infinite	SVR-ADMIN		
Retired/Resigned user data(archiving)	Full	Every last day of the month	2300	I Month/Infinite	SVR-ADMIN ARCHIVE		Full backup
Miscellaneous old user data	Full	As required	Not schedule d	I Month/Infinite	SVR-ADMIN MISC		Full backup
MS SQL Databases (Papyrus & Supplier Databse)							
Roaming User Profiles							
Symantec Endpoint Configuration Database	Full	Every last day of the month	2300				
MS ISA 2006 Configuration Data	Full	Every last day of the month	2300				

Data backed to file and then to tapes using BackupExec							
Data backup name	**Type of backup**	**Scheduling of backup**	**Time backup starts**	**Overwrite/append period**	**Media set name**	**Path to folder**	**Backup strategy**
System state Server ProMIS	Full	Every Saturday		None/none	SS FMS	\\fms-server\backup\serverstate\FMS-S	Weekly full
ProMIS FMS Data Server ProMIS	Full	Every Saturday			Sysvol FMS-S	\\fms-server\backup\FMS\FMS-S	Weekly full
System state Server MOPDC	Presently not backed up						Weekly full
Sysvol Server MOPDC	Full	Every Saturday			Sysvol TERM-S	\\term-server\backup\serverstate\TERM-S	Weekly full
DHCP Server MOPDC	Full	Every Saturday			DHCP TERM-S	\\term-server\backup\serverstate\TERM-S	Weekly full
System state Server COLLAB	Full	Every 2nd Saturday			SS MUNAD-S	\\munadm-server\backup\serverstate\MUNADM-S	Weekly full
System state Server MOPDC	Full	Every 2nd Saturday			SS MAIL-S	\\mail-server\backup\serverstate\MUNADM-S	Weekly full
Sysvol Server COLLAB	Full	Every 2nd Saturday				\\mail-server\backup\serverstate\MUNADM-S	

APPENDIX N – MAILING LISTS

The following table identifies **MDM** Mailing Lists.

NAME	EMAIL ADDRESS	DESCRIPTION/MEMBERS
Manager1	managers1@mopani.gov.za	Senior managers
Managers2	managers@mopani.gov.za	Assistant directors and/or managers reporting to senior managers
Secretaries	secretaries@mopani.gov.za	All secretaries to senior managers and to political offices bearers
AuditCommittee	AuditCommittee@mopani.gov.za	Members of the Audit Committee
Budget Steering Committee	bsc@mopani.gov.za	Budget Steering Committee members
Disaster Management Centre	dmctzaneen@mopani.gov.za	Employees stationed at the Disaster Management Centre offices in Tzaneen
Interns	internships@mopani.gov.za	Interns employed by the municipality through internship programme
LMSecretaries	lmsecretaries@mopani.gov.za	Secretaries to the Municipal Managers of the Local Managers
MayoralCommitttee	mayoralcommittee@mopani.gov.za	Members of the Mayoral Committee of MDM
MunicipalManagers	municipalmanagers@mopani.gov.za	Municipal Managers of LM's and that of MDM
Finanace	finance@mopani.gov.za	Employees attached to Budget and Treasury Office
CommunityServices	communityservices@mopani.gov.za	Employees attached to the Community Services Directorate
CorporateServices	corporateservices@mopani.gov.za	Employees attached to the Corporate Services Directorate
Waterservices	waterservices@mopani.gov.za	Employees attached to the Water Services Directorate
MMOffice	mmoffices@mopani.gov.za	Employees attached to the Office of the Municipal Manager reporting directly to him/her.
EngineeringServices	engineeringservices@mopani.gov.za	Employees attached to the Engineering Services Directorate
MODICT	modict@mopani.gov.za	Members of the Mopani District ICT Forum

APPENDIX O – EMAIL DISCLAIMER

An email disclaimer will be appended to all outbound email. The disclaimer will read as follows:

The information transmitted is only to be viewed or used by the person/s or entity to which it is addressed and may contain confidential and/or privileged material/information. Mopani District Municipality reserves the copyright to all contents of Mopani District Municipality information contained in e-mail messages. The views and opinions expressed in this transmission are those of the sender and do not necessarily represent the views and opinions of Mopani District Municipality. Mopani District Municipality cannot assure that the integrity of this communication has been maintained, or that it is free from errors, malicious code, interception or interference. Under no circumstances will Mopani District Municipality or the sender of this e-mail be liable to any party for any direct, indirect, special or other consequential damages from any use of this e-mail.

GENERAL DISCLAIMER

1. The information provided on this web site is proprietary to Mopani District Municipality and certain clients of and suppliers to Mopani District Municipality.

2. The logos and trademarks included in this web site may not be used for any purpose without the express prior permission of Mopani District Municipality or of the client or supplier to whom such logo or trademark belongs. Enquiries in this regard can be lodged with the Municipal Manager of Mopani District Municipality, via this web site.

3. The information provided is provided without warranty of any sort, express or implied. By using this web site you confirm that you fully indemnify and hold Mopani District Municipality and all of the other parties represented on this web site harmless from all and every claim arising from your use of this web site and the information provided thereon, including special, direct and indirect, and consequential damages. The web site and any web site linked to it are used entirely at your own risk. Links provided on the Mopani District Municipality web site identifies resources and links to other web sites that would appear useful for our readers. The Mopani District Municipality may provide links to other websites only as a convenience and the inclusion of any link does not imply the Mopani District Municipality's endorsement of such sites. Linked websites or pages are not subject to the control of the Mopani District Municipality. The Mopani District Municipality is not responsible or liable, directly or indirectly, in any way for the contents, use, or inability to use or access any linked websites or any links contained in a linked website.

4. You expressly undertake not to use this web site or any other web site linked to it or the information provided on it for any illegal purpose or to transmit or transfer any undesirable material or information of any nature or in any form.

5. Any software provided by means of this web site or any of the web sites linked to it is provided strictly subject to the license agreements and terms and conditions prescribed by the holder of the proprietary rights in such software, and you undertake to honour such rights and prescriptions of the proprietary rights holder concerned.

6. Mopani District Municipality and the Council of Mopani District Municipality or any of its agencies do not necessarily share or agree with the views and opinions published on this web site or any linked web sites, as such views and opinions are published, in many instances, for information purposes only.

7. The Mopani District Municipality web pages are frequently updated and improved. New content will be added as it is available. Although we will attempt to keep information in the Mopani District Municipality web site accurate, the accuracy of the information provided cannot be guaranteed.

8. We welcome third party websites to link to the information that is hosted on these pages. It is expressly prohibited for any person, business, entity or website to frame any page on this website, including the home page, in any way whatsoever, without the prior written approval of the Mopani District Municipality.

9. The Mopani District Municipality reserves the right to change, modifies, add to or remove from portions or the whole of these terms and conditions of use from time to time. Changes to these terms and conditions of use will take effect upon such changes being posted to this website. It is the user's obligation to periodically check these terms and conditions of use at this website for changes or updates. The user's continued use of this website following the posting of changes or updates will be considered notice of the user's acceptance to abide by and be bound by these terms and conditions of use, including such changes or updates.

APPENDIX P - EMAIL CONTENT FILTERING LIST

The following rules have been configured on the email server:

- The following file extensions or attachments are blocked
  - Exe, pif, com, bat, cmd, reg, sys, ini, cpp
  - All movie and music types e.g. Mp3, wav avi, mov, mpg, ogm, Real Audio, windows media player streaming audio, flash
  - All files with pornographic material
  - Pornographic keywords
  - Attachments with pornographic url's
- E-mail exceeding 4Mb in size is blocked
- All spam and unsolicited emails are blocked

APPENDIX Q – EMAIL USE DECLARATION FORM

INTERNET & E-MAIL FORM
SEND THIS FORM TO THE ITO

Please enter your personal details:

First Name	Surname	Employee No
ID No	User ID/Profile	E-Mail
Phone No	Fax No	Building
Department	Section	Town
Floor No	Office No	**Date Required**

☐ **APPLY E-MAIL INDIVIDUAL ACCOUNT**

☐ **APPLY INTERNET USAGE ACCOUNT**

DECLARATION

I understand and will abide by the Municipality **Internet and Electronic Mail Use Policy** and acknowledge and understand that any violation of this policy will be un-procedural, constitutes an act of misconduct and possibly an offence. I further understand that should I commit any violation, further disciplinary actions may be taken against me.

User signature: _____ Date: _____/_____/_____

Head of Section: _____ Date: _____/_____/_____

APPENDIX R – EMAIL USER AGREEMENT

USER CONSENT AND ACCEPTANCE

1. I, the undersigned

   1.1 acknowledge that I have received, read and understand the **MDM** Electronic Mail Acceptable Usage Policy and accept the principles set out in the policy as binding on me;

   1.2 agree that the municipality may from time to time monitor, access and view all communications created, stored, accessed, viewed, received and/or sent by me using the MDM IT system and that I have no guarantee or expectation to privacy in using the department IT system in accordance with the terms and conditions of this policy;

   1.3 Understand and acknowledge that a violation of this policy may result in disciplinary action in accordance with the Municipality's disciplinary procedures, including possible dismissal, as well as civil and criminal liability.

Signed at _____ on this _____day of _____ 20___

_____ _____

NAME **SIGNATURE**

_____

Witness

Appendix S – IT DR TIMELINE DELIVERABLES

Reference	Frequency	Activity
1. Governance	At least twice per year	Summary: Report on DR activity to ITS Senior Leadership Policy Reference: 1.b
	At least every other years	Summary: Review and update DR Policy as necessary. Policy Reference: 1.d
2. Program Development	At minimum, annual updating is required.	Summary: Update existing DR Plans Policy Reference: 2.b
	At least every other years	Summary: Conduct Business Impact Analysis Policy Reference: 2.c
	At least every other years	Summary: Conduct Capability Assessment Policy Reference: 2.d
	At least every other years	Summary: Conduct Risk Assessments Policy Reference: 2.g
3. Emergency Management	Within 45 days of the event	Summary: Complete post-mortem report after outage and recovery response Policy Reference: 3.e
4. Budgeting	Annually	Summary: Complete DR budget Policy Reference: 4.1
6. Vital Records	At least annually	Summary: Review and update published DR plans Policy Reference: 6.e
7. Plan Attributes	Reviewed annually	Summary: Review of backup strategies compliance Policy Reference: 7.c
	Generally not more than 180 days	Summary: Implement defined recovery strategies Policy Reference: 7.f
	Twice per year	Summary: Provide DR training and awareness activities Policy Reference: 7.g

8. Maintenance	Semi-annually	Backup media supporting critical business processes must be tested Policy Reference 8.d
	Within 60 days	Summary: Reviews are required after a test to correct exposed deficiencies Policy Reference: 8.d
	Within 60 days	Summary: Complete Plan revisions after the test review. Policy Reference: 8.e
	Annually	Summary: Conduct DR maintenance activities Policy Reference: 8f

ANNEXURE T – RECOVERY TIER CHAT

Recovery Tier Chart ranks IT services by business-defined recovery requirement during the Business Impact Analysis process (see below for MDM Recovery Tier Chart):

TIER	CRITICALITY	RTO	RPO	TYPE OF DR HW	REPLICATE OR TAPE	DR PLAN	CONFIG
0	Self-Healing		PoF	Dedicated	Replicate	Yes	Hot/Hot
1	Mission Critical		PoF or Intra-Day	Dedicated	Replicate	Yes	Hot/Warm
2	Highly Critical	< 72 hours	Intra-Day or SoD	Dedicated	Replicate or Tape	Yes	Hot/Cold
3	Critical	< 7 days	SoD	Quick Ship	Tape	Yes	N/A
4	Non-Critical	< 2 weeks	LC	Determined ATOD	Tape	Yes	N/A
5	Deferrable	> 2 weeks	LC	Determined ATOD	Tape	No	N/A

Risk Assessment (RA) is the initial steps of Risk Management which analyses the value of the IT assets to the business, identifying threats to those IT assets, and evaluating how vulnerable each IT asset is to those threats.

Service Manager is the owner of a service as defined by one of the user or technical catalogs.

Technical Service Catalog maps technical activities of the User Services Catalog to select ITO systems and applications. This mapping helps understanding of how changes in these services impact the users.

ANNEXURE U - OFFICIAL WEB CONTENT UPDATES SCHEDULE

NAME OF DOCUMENT (e.g. 2012/13 MTEF Budget)	TYPE OF DOCUMENT (e.g. Budget Document)	SOURCE DIRECTORATE (e.g. BTO)	RESPONBIBLE OFFICIAL (e.g. Assistant Director-Budget & Reporting)	DUE DATE (e.g. 30/05/2012)	SUBMITTED IN TIME? (Yes or No) DATE	PUBLISHING DATE (e.g. 05/06/2012)	PUBLISHED IN TIME (Yes or No) DATE