Molemole Municipality

IT AND INFORMATION MANAGEMENT SECURITY POLICY

		Version Control	
Version	**Approved Date**	**Resolution No**	**Responsibility**
01	24 January 2013	OC03/2012 (6.7/24/01/13	Corporate Services Department

TABLE OF CONTENTS

PREAMBLE

1.1 Molemole Local Municipality is a service-orientated public entity whose legislated mandate is to provide services to residents and in pursuit of the mandate make use of various communication methods and mechanisms;

1.2 Legislation prescribes that the municipality must establish controls and systems to regulate the appropriate and efficient use of municipal resources;

1.3 This security policy indicates senior management's commitment to maintaining a secure Network, which allows the IT Staff to do a more effective job of securing the municipality's information assets.

1.4 This policy seeks to provide a framework and set standards aimed at ensuring that the ICT hardware and software assigned to municipal officials are used appropriately and at minimum costs to the municipality.

1.5 This IT Security policy has been drawn from the extensive experience of best international practices and is based upon the foundation of ISO **17799, BS 7799 and COBIT.**

1. PURPOSE AND OBJECTIVES OF THE POLICY

1.1 The objective of this policy is provide a guideline for the application of IT Security Management in order to protect municipal data, network systems and applications against all manner of threats of confidentiality, integrity and availability.

1.2 To provide documented measures to protect municipal assets against accidental or unauthorized modification, disclosure or destruction of automated data processing activities;

1.3 To set guidelines for allocation and usage thereof of IT hardware and software to officials and other contracted individuals.

1.4 To provide a framework for formation of Municipal IT Steering Committee

1.5 To provide a framework for drafting an effective IT Security program that will enable IT Personnel to detect anomalies in network traffic and take the necessary proactive steps toward mitigation.

1.6 To identify the rules and procedures that all persons accessing computer resources must adhere to in order to ensure the confidentiality, integrity, and availability of data and resources.

1.7 To ensure that access granted to computer services and data is based on business requirements, and that access granted is consistent with job descriptions and requirements.

1.8 To safeguard municipal information in such a way as to ensure data recovery in case of accidental loss of data.

2. RESPONSIBILITIES

2.1 Corporate Services Department is the implementing agency of this policy;
2.2 A municipal IT Steering Committee should be established whose main function is to monitor adherence to all the provisions enshrined in this policy.
2.3 The IT Steering Committee should be comprised of officials who have a clear understanding of Information Technology trends.
2.4 Where possible, workshops or training should be organized for members to ensure they have an up to date understanding of IT trends, general and for government in particular.

3. DEFINITION OF TERMS

Terminology	Definitions
Antivirus software	A software that helps to prevent a computer from virus attacks
COBIT: *Control Objectives for Information and Related Technologies*	A framework for information technology management and IT Governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
Data Recovery	A process whereby information that is backed up is restored to its original location after accidental loss
Firewall	A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set.
HTML	Hypertext Markup Language
Internet Hyperlink -	Automatic link to a URL
Internet Service Provider	An organization that provides internet service to other organizations, e.g. MWEB, Telkom, etc.
ITO	Information Technology Officer
NDIS	Network Driver Interface Specification
Off-site backup system	A backup system that is installed away from the Municipality to ensure data recovery in case of disasters
Patches	A patch is a piece of software designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities[1] and other bugs, and improving the usability or performance
Personal Account -	An Account given to officials to give them access to municipal network
Remote Access	Connection to a data processing system from a remote location, for example through a virtual private network
Removable storage device	A removable disk on which data may be stored. Usually refers to CDs, Tapes, & floppies, etc
URL -	Uniform Resource Locator

4. LEGISLATIVE REQUIREMENTS

4.1 This policy is governed by the following legislative imperatives:

a) The constitution of the Republic of South Africa, 1996 (act 208 of 1996)
b) Municipal Finance Management Act, 2003 (act 53 of 2003)
c) Municipal Systems Act, 2000 (act 32 of 2000)
d) State Information Technology Act (Act no 88 of 1998).
e) Protection of Information Act (Act no 84 of 1982).
f) Promotion of Access to Information Act (act 2 of 2000)
g) Minimum Information Security Standards (MISS), Second Edition March 1998
h) National Archives Act, 1996 (Act 43 of 1996)
i) Control Objectives for Information and Related Technologies(COBIT)

5. SCOPE AND TARGET AUDIENCE

5.1 This policy applies to:

5.1.1 all permanent, contractual and non permanent employees of the municipality whose functions may require access to municipal IT networks, applications and servers;

5.1.2 All permanent, contractual and non-permanent officials/ individuals/ organizations that have been given municipal IT Assets like Laptops, Desktops, Printers and other related devices

5.1.3 All permanent, contractual and non permanent employees/individuals/ organizations who have access to electronic mail applications and operating systems of the municipality.

6. POLICY STATEMENT

6.1 ACCOUNTABILITY OF ASSETS

6.1.1 It is the responsibility of each Departmental heads, Manager, officials and authorized contractor to ensure that all the municipality's assets used to access the municipality's IT infrastructure are adequately accounted for. Any information, changes in ownership, allocation of these assets, changes in configuration and usage outside of the municipality's premises must be communicated to the Manager IT.

6.1.2 An inventory of assets must be maintained by the Manager IT to ensure that effective security protection is implemented. This inventory should be aligned to the overall asset register and policy of the municipality.

6.1.3 Critical IT assets should be identified and appropriately documented. These assets include, but are not limited to:

6.1.3.1 Network interconnection components like: routers, switches, hubs, etc.
6.1.3.2 Servers: Mail, File, Web
6.1.3.3 External Components: modems and remote access servers
6.1.3.4 External Components: authentication servers and firewalls
6.1.3.5 Personal Computers and laptops

6.1.4 The Manager IT must keep a proper documentation concerning the municipality's critical IT assets, which should cover the following:

6.1.4.1 Identification: location, supplier maintenance contracts and persons using the assets
6.1.4.2 A short description of every available critical IT asset explaining its function and use.
6.1.4.3 Technical configuration documentation of each asset
6.1.4.4 Information on linkages with other IT assets
6.1.4.5 The Model, type and Serial number

6.2 PERSONAL RESPONSIBILITY FOR SECURING INCIDENT REPORTING

6.2.1 All users of IT assets/equipment must take responsibility for reporting the different types of incidents that might impact on security of municipal assets, e.g. security breach, weakness or system malfunctioning.

6.2.2 A security incident is any incident which may affect or has affected:

a) The confidentiality of the municipality's information (electronically stored).
b) The integrity of the municipality's data
c) The availability of municipality's IT systems

6.2.3 These incidents may include, but are not limited to:

a) Virus attacks which might affect the municipal servers
b) Resource/network attacks or Hacking
c) Operational incidents
d) Loss incidents

6.2.4 The Manager IT must develop an Incident reporting template to be used for recording of all incidents and actions taken to remedy them. The Manager IT must provide quarterly reports to Management on all incidents reported, remedies as well as a recommendation on how the incidents can be avoided in the future.

6.3 PHYSICAL AND ENVIRONMENTAL SECURITY: IT (SERVER) ROOM

6.3.1 All IT facilities supporting critical or sensitive municipal activities should be housed in secure areas which are only accessible by properly authorized individuals and protected from intentional and accidental damage.

6.3.2 IT Equipment should be located in an area which is safe and healthy, enables operational functionality and access to maintenance and the storage should have adequate air circulation.

6.3.3 All Bulk and heavy equipment like servers must be housed in floor standing cabinets.

6.3.4 Anyone entering the IT Server room must get preauthorization, maintain cleanliness of the room, dispose of all rubbish and refrain from eating or drinking within the room. A copy of these practices must be placed at the wall of the room for staff cleaning the server room.

6.3.5 A periodic program of specialist cleaning should be done in all IT rooms and the frequency of cleaning must be in line with the environmental regulations and also include floor (in case of raised floor) and above the ceiling (in case of false ceiling)

6.3.6 Cabling must be kept tidy, cable trays should be used where applicable, and all cables must be terminated in floor standing cabinets and labeled for ease of identification.

6.3.7 Server rooms must be physically secure and access to it should be through an electronic system which provides a record of successful and failed attempts at entry. All failed entry attempts should be investigated by the ITO and appropriate disciplinary measures and remedial measures be taken to address them.

6.3.8 Use of appropriately rated power outlets is necessary to ensure safe and secure connections and overload protection must also be supplied.

6.3.9 Any changes or upgrades to the equipment in the IT room should be followed by a proper electrical loading. A fully functional UPS protection must be installed in the IT room and where it is practical backups should be generated.

6.3.10 IT Server rooms must be protected by an early warning mechanism for fire consisting of smoke detectors or heat detectors integrated into the building fire alarm system which should raise an audible alarm and cut the power supply to the room on activation.

6.3.11 An automatic fire extinguishing system that can be within a set time must be installed in the IT room. This fire extinguishing system must also be operational manually when staff is present.

6.3.12 IT rooms must have an air conditioning system that operates 24 hours, 7 days a week and should be designed to keep the room to within the IT manufactures' recommendation for temperature and humidity throughout the year.

6.3.13 The ITO must monitor temperature, humidity, power and cleanliness in IT rooms to anticipate, if any, potential problems with air conditioning equipment and power supplies.

6.3.14 Adequate lighting should be maintained at all times in the IT rooms.

6.3.15 The ITO will, with the express concurrence of his/her Senior, only give authorization for accessing IT rooms for the following purposes:

a) Operation, housekeeping, testing or storing of equipment;
b) Maintenance or upgrades to IT Equipment or cleaning of environmental facilities;
c) Management or Audit;
d) A register of all authorization granted as well as reasons for granting entrance must be kept by the ITO;
e) IT rooms must NEVER be left unattended unless they are fully secured to prevent unauthorized entry;

f) Any official who suspect that there is any form of security breach must immediately report to ITO to attend to it. This may include, but not limited to: unauthorized entry, doors left open, locks not working, fire exit glasses broken, security codes divulged to unauthorized personnel or lost keys.
g) 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.
h) ANYONE FOUND TO HAVE ENGAGING IN PRACTICES THAT MAY LEAD TO SECURITY BREACH WILL FACE DISCIPLINARY HEARING WHICH MAY LEAD TO DISMISSALOR IN SOME CRITICAL INSTANCES, BE SUBJECTED TO CRIMINAL PROSECUTION.

6.4 SECURITY OF REMOVABLE MEDIA

6.4.1 All backup media must be stored in a secure location in an environment conducive to storage of magnetic media and operational use;
6.4.2 The ITO must ensure that media used for backups and archiving does not exceed the manufacturers' guidelines on useful lifetime;
6.4.3 All media located off-site of the municipal premises must be logged in and out to ensure that all copies can be located and audited;
6.4.4 Backup media transported to off-site storage must be transported in a reliable transport or couriers with adequate insurance cover; should be sufficiently packaged (tamper proof) to avoid physical damage and be held in secure containers;
6.4.5 All formal backup and archive media should be clearly marked;
6.4.6 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;
6.4.7 A clear and approved backup procedure must be developed to provide proper guidelines on backup frequencies, backup restore procedure for off-site backups and disposal of backup media.

6.5 ACQUISITION AND ALLOCATION OF COMPUTER EQUIPMENT

6.5.1 At the request of the employee's manager, accompanied by a signed appropriate Application for IT Equipment Form, computer equipment may be allocated or procured and an employee may have access to computer-based services, including software installation, user account, shared printer, e-mail and web services. These features are provided to assist officials to fulfill his/her official duties and/or business activities. The ITO will set the qualifying criteria for each official;
6.5.2 New equipment will be procured only if current equipment does not comply with the minimum standards set for the computer equipment;
6.5.3 In cases where an employee requires the allocation of non-standard equipment or software to fulfill their duties effectively, the employee's senior manager must make a recommendation in the form of a motivated submission to the Municipal Manager who must give authority;
6.5.4 The submission must include the specifications and cost of the software or equipment required;

6.5.5 The ITO will advise on the legal implications of procuring the software and licenses thereof.

6.6 STANDARDS

6.6.1 To make for cost-effective use of equipment and software, the Municipality will standardize on a core set of software and hardware product requirements and the specifications will be set and revised from time to time by the Manager IT.

6.6.2 Desktop computers - Users may only request new computers if their current computers do not comply with the minimum hardware specifications set by the ITO. As far as is possible, users will be issued with a computer that meets their preferred specifications, subject to financial resources of the municipality;

6.6.3 When the standard is raised, computers below the standard will be upgraded by the ITO or new computers will be procured if these computers have reached their economic lifetime;

6.6.4 To control maintenance cost, no other software may be installed without the written approval of both the user's Senior Manager and the Manager IT.

6.6.5 Only hardware or software related to an official's area of responsibility shall be installed on the computer;

6.6.6 All computers procured by the municipality for officials must be prepared by the ITO using municipal network systems to install software and create users on the domain system.

6.7 ACCESS CONTROL

6.7.1 All business requirements for access control should be defined and documented by the Manager IT;

6.7.2 Proper procedures for addressing access rights should cover all stages in the life-cycle from initial registration of new users to their de-registration. Users will only be given access to those functions and applications necessary to perform their assigned duties;

6.7.3 The Senior Manager: Corporate Services or any authorized official should periodically conduct a formal review of users' access rights with specific focus on those given privileged rights. Monthly reports of users and administrators' activities should be kept;

6.7.4 The ITO should ensure that user access rights to the municipality's systems are in line with their needs, are clearly defined in a formal request, authorized by user's Superior when user's responsibilities are changed and timely removed when a user leaves the municipality;

6.7.5 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;

6.7.6 Appropriate segregation of duties, specifically allocated and defined in writing, shall apply;

6.7.7 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.

6.7.8 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.

6.7.9 The access control system shall update an audit trail of all authorized and unauthorized efforts to gain access to the computer systems. Unauthorized access attempts shall be considered a breach of security.

6.7.10 Passwords shall be individual and exclusive, and shall not be disclosed without authorization in forced exceptional cases, and without documenting the incident. Unauthorized disclosure of passwords shall be considered a breach of security.

6.7.11 A password policy/procedure should be developed to ensure only authorized users gain access to the network. Users should be prompted to change their passwords at intervals to ensure continued credibility of access rights.

6.8 SECURITY REQUIREMENTS FOR IT PROJECTS

6.8.1 An analysis of security requirements must be carried out at the requirements analysis stage of each business application development project. Statements of business requirements for new business applications, or enhancements to existing business applications must specify the requirements for security controls. Such specifications normally focus on the automated controls to be incorporated in the system, but the need for supporting manual controls must also be considered. These considerations must also be applied when evaluating software for business applications.

6.8.2 Security controls must reflect the business value of the information assets involved, and the potential business damage that might result from the failure or absence of security.

6.8.3 The Manager IT must develop a formal user registration and deregistration process which should include procedures, periodic check for redundant ID's and also ensure access rights are in line with functions, rank and responsibilities of each user.

6.9 SECURITY MONITORING

6.9.1 The Senior Manager: Corporate Services or the duly designated official should perform formal periodic security monitoring on the following:

a) Access privileges
b) Security access logs
c) Redundant ID's

6.9.2 A report detailing the authenticity of access rights issued should be compiled on a quarterly basis and presented for approval by the IT Steering Committee.

7. SYSTEM DEVELOPMENT AND MAINTENANCE

7.1 Introduction

7.1.1 It is the municipality's commitment that an adequate change control process and procedures should be implemented to provide reasonable assurance that any changes made to the municipality's systems and applications in the operational environment are always identified, properly authorized, tested, approved, implemented and documented.

7.1.2 At the minimum, the change control process should include the following components:

a) Initiation and approval of a change or development project
b) Product development
c) End user acceptance testing
d) Release planning
e) Maintenance and Support

7.2 INITIATION AND APPROVAL OF A CHANGE OR DEVELOPMENT PROJECT

7.2.1 Any software changes or new developments must be formally initiated through formal change requests. All change requests issued should be checked for validity, duplicates and formally approved by the Management Committee of the municipality

7.2.2 Only formally **APPROVED CHANGE REQUEST FORMS** should be considered as triggers for initiating development projects.

7.3 PRODUCT DEVELOPMENT

7.3.1 Product development should include the following components:

a) Requirements analysis
b) Developments approach (methodology, standards)
c) Module testing
d) System testing

a) Requirements analysis

Security countermeasures are substantially cheaper and more effective if incorporated in application systems at the requirements specifications and design stages. All security requirements, including the need for fallback processing, should be identified at the requirements phase of a project, justified, agreed and documented as part of the overall business case for an information system

b) Development approach

Changes made to software must be performed in a separate environment from the production environment. A development methodology, containing standards and guidelines for system development by IT officials should be available and strictly followed. Control should be in place to assure that support programmers are given access only to those parts of the system that are necessary for their work.

c) Module testing

Every individual programmer is responsible for the performance of module tests on the programs developed. Module tests need to be performed in an environment separate from the production environment. They need to be formally approved by the IT Steering Committee before they are introduced.

d) System testing

System testing should be performed in a separate environment from the production environment. Formal system test plans and scripts should be drawn up based upon the results of the requirements analysis. System testing usually requires test data to be as close as possible to the live data. Test data should be protected and controlled. The use of live personal data should be avoided. If such data is used it should be depersonalized before use. System test results should be formally reported and approved by the IT Steering Committee.

e) Acceptance testing

Acceptance testing should be performed by end users in a separate environment from the production environment. Formal acceptance test plans and scripts should be drawn up based upon the results of the requirements analysis. Acceptance testing usually requires test data to be as close as possible to the live data. Test data should be protected and controlled. The use of live personal data should be avoided. If such data is used it should be depersonalized before use. Acceptance test results should be formally reported and approved by the IT Steering Committee.

f) Release planning

Formal procedures for the implementation of new product releases should be available and must ensure that only tested and formally approved programs are taken into production environment. Special attention should be given to: *End user sign-off including sign off for specific security requirements; Technical change management; and program transfer from test to production environment only to be executed by authorized officials.* A proper maintenance and support plan must be developed in order to avoid persistent downtimes after the system has been fully rolled out. Where possible these maintenance guidelines should be pasted at Server room.

8. FIREWALL AND PERIMETER SECURITY

8.1 The municipality's secure network is protected from the internet and non-secure networks with firewalls and intrusion prevention systems.
8.2 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.
8.3 Wireless devices and VPN access are not allowed on the municipality's network, unless provided for in exceptional cases which should be documented by approved by the IT Steering Committee and ITO.
8.4 RAS dial-back shall be activated and only to a pre-defined and authorized telephone number.
8.5 VPN network extensions are only permitted making use of secure tokens, managed and supplied by IT SECTION.

9. END-USER COMPUTING POLICY

9.1 USE OF COMPUTER EQUIPMENT FOR OFFICIAL PURPOSES

a) Computer equipment is issued to employees for official duties and for Municipality's business or activities sponsored or authorized by the Municipality;
b) Officials should refrain from incurring municipal IT resources and time for personal gain. This includes but not limited to: website surfing, personal exchange of mails or any matter connected therewith;
c) Officials should not cause the municipality to incur costs related to personal use of IT equipment
d) 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.
e) The Management Committee of the municipal reserves the right to determine the extent of Network and/or Internet services to be afforded to officials. Officials shall not be unreasonably denied access to internet access if it can be proved that those officials' line of work requires access to internet.

9.2 STORING OF MATERIAL ON COMPUTER

a) 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 recorded audio sounds;
b) Officials should refrain from saving personal information on municipal IT equipment. Regular audits will be conducted as and when the IT Unit deems necessary to ensure compliance to security guidelines provided in this policy;
c) Storing of the following material is expressly prohibited: Discriminatory, intolerant or derogatory matter 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.

d) Unless computer equipment needs to run after hours, users must switch off the equipment at the end of each working day.
e) If an employee's computer is not logged out it is a security breach to the Municipality and switching off of computer equipment is considered best practice to reduce the risk of fire, saving energy and ensure that any documents that employees have worked on are properly closed and ready for backup.
f) Employees are advised to save all computer-based work they produce on the main network of the municipality. The Municipality provides employees with network-based storage and if employees are producing work that needs to be shared, the employees should ask the ITO to set up a shared folder on the network.

9.3 USE OF MUNICIPAL NETWORK BY OUTSIDE STAKEHOLDERS

a) Anyone, other than the duly appointed officials (including consultants) of the municipality should get authorization from the Manager: Corporate Services by filling an authorization form at least three days before the day of access to municipal network systems;
b) The authorization form should specify the following information:
    i. The name of Service Provider, Person(s) requiring access;
    ii. The Name of company representative requiring access to the system;
    iii. The total hours required for access;
    iv. The reason for requiring access to the municipal network;
    v. Any configurations that will be done on the software/program;
c) Approval for accessing to the network will be enforceable only if it is done by the Accounting Officer.
    i. Printers will be allocated to officials depending on the specific requirements or confidentiality of their work. Colour printers will be allocated to officials at Senior Management and Divisional heads level who frequently needs to print colour documents; other officials will be required to use the central (communal) printer.

9.4 INSTALLATION OF HARDWARE AND SOFTW ARE

a) Only the ITO is authorized to install or copy software programs on computers allocated to municipal officials;
b) A user may be held personally liable for any damages and legal costs, if he or she copies software illegally onto the municipal computer or for installing municipal software onto their personal computer;
c) If the user discovers any offensive material on his/her computer, or on the network, the employee should report it to the ITO to investigate and take appropriate action.

d) There are circumstances where users will be allowed to provide their own software, or software licensed to a service provider. In this case, the user's Manager must provide motivation and documentary proof that the employee holds a valid license before the software will be installed onto the municipal computer. 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 for the use of personal software;
e) The municipality will normally own the copyright for software written "in-house", by the Municipality. Such software may be used within the Municipality without a license. But, users must still have these programs installed by authorized support staff. Employees are still committing an offence if they copy, for non-official use, software owned by the Municipality.

9.5 CODE OF CONDUCT FOR USING MUNICIPAL IT RESOURCES

9.5.1 All users of municipal IT systems and infrastructure must adhere to the following code, failing which disciplinary action shall be preferred against them:

a) Employees shall take care to use all computer equipment and resources in a responsible, ethical and lawful manner;
b) No employee should waste computer resources or unfairly prevent others from the use of such resources;
c) Employees may not use the Municipality's computer facilities to:
ii. Play games or run other entertainment software,
iii. Save files containing images, music, sound or video onto Municipal 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 and an authorization should be obtained from the IT Office. This is usually the C: drive;
iv. Make or store illegal copies of material protected by copyright. This includes software programs and publications, in whole or in part;
v. Back up their personal local hard drives onto Municipality servers
vi. Print large documents if there is a viable on-screen alternative;
vii. and Print personal or non-municipal information using municipal printers

9.5.2 Employees have a duty to take good care of the equipment issued to them. This is particularly relevant to staff who use portable equipment such as laptops, notebook computers and memory sticks;

9.5.3 Users may not transmit personal opinions as those of the municipality, nor make any statement that may be construed to be a municipality's statement.

9.5.4 The following disclaimer should be included as a suffix to all e-mail messages to addressees external to the municipality:

The information contained in this communication is confidential and may be legally privileged. It is intended solely for the use of the individual or entity to whom it is

9.5.5 Employees may not lend the equipment issued to them for whatever reason to anyone for any reason whatsoever without the express permission of the ITO. An official who lend any of the allocated IT equipment in term of 9.2.1 above shall hold full responsibility if the equipment is damaged or stolen;

9.5.6 The municipality has a right to recall the equipment if it can satisfy itself that an official is lending the gadget to unofficial persons;

9.5.7 Employees issued with laptops are automatically given the permission to take them home but should fill in the equipment removal control form available at the ITO;

9.5.8 Employees may not install, move, and tamper with computer equipment. Only authorized support personnel may move, upgrade or repair computer equipment or make changes to system configurations;

9.5.9 Employees may not remove, install or tamper with any internal component of a computer or the equipment that may be attached to it (e.g. printer).

9.5.9.1 Employees may not move computer equipment to another room, or site - unless it is specifically designed to be carried around (e.g. notebook computers). Employees may not swap equipment with other users as moving or swapping equipment will create inconsistencies in the asset register. Employees should contact the ITO, (who must inform the Asset Manager) to arrange for the equipment to be moved or installed for them.

9.5.10 Users may open a printer to remove or replace paper as well as a toner or print cartridge. Should an official not be able to do so he/she must call the IT Officer for assistance.

9.5.11 Officials must report to ITO if they need a replacement or upgrading of the IT equipment so that he/she can test the equipment to justify the need for replacement

9.6 <u>LOST, DAMAGED OR STOLEN EQUIPMENT</u>

Officials are expected to take due diligent care of the IT equipment(s) assigned to them.

9.6.1 If an employee loses or damages equipment, software or data that belongs to the Municipality, the employee must promptly report in writing to his/her Head of Department and the ITO within 24 hours of existence.

9.6.2 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 and keep the case number for investigation purposes.

9.6.3. In terms of the Municipality practices and policies, the user must provide the report and include the following information in case of theft, damage or loss:

a. Serial number of the IT Asset that was stolen or lost

b. Case reference number of the South African Police Service (SAPS)
c. Date it was stolen and a short description of what happened
d. The ITO will then change the Status of the item/s to "Stolen/Damaged/Lost"

9.6.4 If it is proven that the reason for loss or theft of the IT Equipment was due to negligence on the part of the official, the said official will be ordered to replace the IT Equipment or the municipality will replace the equipment and recover costs from the employee's salary.

9.6.5 The Municipality may replace or repair the stolen equipment by claiming from its insurance in which case the official who lost or damaged the equipment shall pay all excess costs associated with those repairs or replacement.

9.7 TERMINATIONS, TRANSFERS AND RESIGNATIONS

9.7.1 When an official resigns, retires or is dismissed from the municipality he/she must return all IT Assets in good working condition, wear and tear excepted.

9.7.2 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 department of the municipality.

9.7.3 The ITO in consultation with Asset staff will check if the content on the form completed by the user corresponds with the IT asset register and the physical IT assets before signing off.

9.7.4 The Municipality reserves the right to deduct monies from the pension claims of the official if the user is unable to adhere to the above stipulations

10. DO N'T S AND DO'S

You are not allowed to:

a) BRING YOUR HOME COMPUTER ALONG TO THE OFFICE.
b) MOVE YOUR COMPUTER WITHOUT INFORMING THE INFORMATION TECHNOLOGY UNIT.
c) PUT YOUR COFFEE/TEA CUP ON TOP OR CLOSER TO YOUR COMPUTER.
d) DISCONNECT YOUR PC FOR A REASON NOT KNOWN TO THE IT UNIT.
e) INSTALL A THIRD PARTY SOFTWARE OR NON-STANDARD SOFTWARE, UNLESS AUTHORIZED TO DO SO.
f) INSTALL COMPUTER GAMES OR OTHER ENTERTAINMENT SOFTWARE.
g) REPAIR OR PERFORM ANY FORM OF UPGRADE TO THE COMPUTER EQUIPMENT.
h) SWAP COMPUTER EQUIPMENT WITH OTHER OFFICIALS.

You must

a) SWITCH OFF YOUR COMPUTER WHEN YOU KNOCK OFF.
b) BE LOGGED INTO THE NETWORK WHEN USING A COMPUTER.
c) OBTAIN A PERMIT BEFORE TAKING AN EQUIPMENT OFFSITE, UNLESS IT IS A NOTEBOOK OFFICIALLY ALLOCATED TO YOU.
d) ALWAYS KEEP YOUR DESKTOP COMPUTER TIDY.
e) INFORM IT UNIT IF YOU SUSPECT THERE IS SOMETHING WRONG WITH YOUR EQUIPMENT BEFORE IT IS TOO LATE.
f) REPORT ANY UNLICENSED OR SUSPECTED NON-STANDARDIZED SOFTWARE TO THE ITO

COMMENCEMENT AND REVISION

9.1 This policy takes effect immediately after approval and will be reviewed after 3 years from the date of approval. 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 the municipality by way of e-mail or memo.
9.2 Amendments will only be binding after approval by majority members of Council

ANNEXURE A: ICT EQUIPMENT DATABASE REGISTER FORM

1) **I, the undersigned, acknowledge that I am an Official** ☐
Councillor ☐
Contractor ☐

Of Molemole Municipality and hereby declare:

Mlm code _____ Brand name _____ Asset category _____

Date Purchased _____ Assigned user _____ Date Assigned _____

Position _____ Office Based _____ Department _____

Purchase Price _____ License no _____

Model _____

SPECIFICATION

Memory size _____ CPU size _____ CD Drive _____

Stiffy Drive _____ Monitor Type _____ Keyboard _____

3G Card _____ Printer Asset code _____ HDD Size _____

Mouse _____

As a registered User I am aware of and undertake:

a. To take reasonable care to prevent the willful or negligent loss of or damage to the equipment;
b. The following factors should be considered:
    i. In the event of damage to the equipment at any time while it is in my possession, I agree to inform the ITO within 24 hours;
    ii. To pay the cost of repairs of all damages or replacement to the equipment caused by the lack of due care, negligence, or misuse;
    iii. To make use of the Municipality Support Services of the ITO for the maintenance of the equipment;
    iv. To adhere to all the Municipality IT Asset and Inventory Control Procedures, the Security Division's policies and measures in this regard, as well as the Financial Circulars pertaining to the loss of or willful damage to equipment.
    v. To notify the ITO as per IT ASSET RELEASE FORM of my intention to move the equipment should it become necessary for the performance of my duties
    vi. To connect my computer to network every time I am in the office for backup and virus protection
    vii. 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.
c. Failure to return the equipment may result in the municipality taking legal action to recover said equipment and recover any damage thereto, or recover the depreciated value thereof, at their sole discretion.

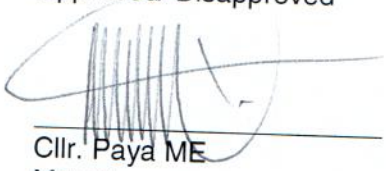
2. **With reference to the Support, Maintenance and IT Asset Control policies and the Procedures and standards of equipment of the Municipality, I also accept:**
    a) That all equipment will be configured and maintained by the Municipality only.
    b) That equipment may not be exchanged between Users or workstations without consent of ITO.
    c) That as the User I shall not copy my personal information into the municipal computer
    d) That I shall not lend this equipment to any unauthorized person(s) without the approval of the council (in case of Councilors) or Municipal Manager (in case of officials).

e) That I shall take responsibility of whatever kind deemed to be necessary by the municipality should I not adhere to provisions of clause 3.

Approval of the Policy

This policy shall be effective from the date of approval and shall be reviewed after three years from the date of approval or should the need arise.

Approved/ Disapproved



Cllr. Paya ME
Mayor

31/05/2022
Date