EMAKHAZENI LOCAL MUNICIPALITY

ASSET MANAGEMENT POLICY

Approval

DOCUMENT:	**ASSET M ANAGEMENT POLICY**		
Copy Number:	**Master Copy**		
Compiled by:	Niall Carroll	**Reviewed by:**	
Compilation Date:	August 2013	**Review Date:**	
Version:	V 1.03	**Revision:**	
Distribution:	All	**Classification:**	
Document Release Approval		**Document Acceptance**	
Releasing Authority: Deputy Manager: ICT	ICT	**Acceptance Authority:**	Council
Date Released:		**Date Accepted:**	
	Signature:		**Signature:**

DOCUMENT CONTROL

0.1 Revision Record

Revision	Date	Change Record	Changed By
1st	April 2009	New ICT Policy – submitted to Council	N Carroll ICT
2nd	March 2013	Reviewed and updated	N Carroll ICT
3rd	August 2013	Re formatted layout	N Carroll ICT

0.2 Issue Control

This policy is issued by the Corporate Services Department on behalf of Emakhazeni Local Municipality, to whom any change requests or queries should be directed. The review life for this document is 12 months.

0.3 Distribution

Copy No.	Name	Title	Organisation
Master			
01			
02			

The MASTER for this document is held electronically and only signed copies are valid. An unsigned, printed document is not copy controlled and is to be used for information purposes ONLY, as it will not be automatically updated. It is therefore the responsibility of the reader to ensure that it is a currently valid copy.

Table of Contents

ASSET MANAGEMENT

PURPOSE OF THE POLICY

The purpose of the policy is to assist in governing and controlling assets specifically in respect to Information Technology and to guide in the management of such assets.

1. USAGE OF INFORMATION TECHNOLOGY ASSETS

1.1. All equipment and software that are used in Information Technology are seen as assets to the municipality and must be properly managed and controlled to ensure optimum usage of such equipment. All Information Technology and Information Technology related assets should be controlled according to relevant laws, policies and instructions governing the control of such equipment for especially government organizations.

1.2. All Information Technology equipment and software acquired by the Local Municipality must be used by and for the Emakhazeni Local Municipality and the mandate that the municipality has in accordance with the laws of the country. The use of these assets must benefit not only the municipality but also the community that the municipality is instructed by law to attend to and oversee. The length of the usage should not be less than three (3) years. A common Information Technology solution should last between three (3) and five (5) years provided there is no dramatic change in technology.

1.3. The equipment and software should be used responsibly and within the manufacturers specifications and in no way be abused for personal gain, roughly handled to such an extent that the equipment may be damaged or use to further an organization other than the government and municipality.

1.4. Components of the computer hardware may not be removed from the computers unless the computer fails due to normal usage or an act of God such as lightning or floods that renders the computer as a whole unusable but components there-of still usable. Such components should be allocated to government computers only and should be installed to improve such equipment where improvements are necessary and may not be sold or given to private individuals or organizations. This may include RAM chips, hard disks, processors (CPU's), cables, and even VGA adapters (screen cards).

1.5. All computer equipment that reached the end of life should be treated in accordance to government and National Treasury policies and procedures and GAMAP principles on equipment and assets reaching the end of life span. All equipment must be sold after properly written off and if there is no use of any sort for it in the organization such as backup units while a computer is being repaired or community development centres or similar projects are run as part of the municipality's mandate to uplift and improve the community through such projects.

2. MANAGEMENT OF ASSETS AND RECORDKEEPING

2.1. All Information Technology assets must be listed in a register or inventory in either manual or electronic format and should be updated regularly. This inventory must be verified and spot checks on equipment should be done along with regular services. Because of the nature of Information Technology equipment and software it is very important to maintain strict control over it as abuse and theft can easily be committed. Software can be used on many computers without traces of such theft until checks are done. Using software illegally can result in all parties involved being charged with software piracy and theft and the onus is then on them to proof otherwise. Hardware components can show up easily as being stolen by checking system configurations against what was issued to personnel or installed on their computers. Common items stolen are RAM, cables and hard disks. In some cases, processors (CPU's) have been stolen and replaced with one of a lower performance level.

2.2. A network and computer management program should be installed to keep track of computer and file server hardware configurations and indicate where changes have occurred on computers and file servers. It is not uncommon for such items to be stolen or taken and replaced by lesser components. Such programs are available to audit such equipment and report any changes according to the compiled configuration inventory for a computer or file server.

2.3. Regular audits should be carried out on computer equipment to control and manage Information Technology assets. Reports should be made out to the Head of the Department responsible for Information Technology and the report must then be tabled to the Executive Committee to provide feedback. It should also serve as information on the management and control over assets within the municipality and govern any action against

people guilty of contravening control and management policies and instructions over assets.

2.4. A regular stock take should also be held at least annually to ensure that the inventory held on the Information Technology equipment is still in order and that the computers are used where indicated. It should also reflect the status of the equipment and devaluation should be recorded for the equipment and the time it is in operation in accordance with the GAMAP principles. The stock take should also indicate according to the devaluation of the equipment the timeframe left in operation for this equipment.

2.5. Software must also be controlled and during this stock take the relevant information must be gathered to see whether all licensing agreements are adhered to. Where there are discrepancies it should be resolved in order to ensure that all products are properly licensed and these products are in use on the computers indicated and fully licensed. Because software just go outdated and are replaced by newer, more powerful software the municipality must ensure that the best usage is made of software as it can be a costly investment. The software should be standardized and the same irrespective of when and where the computer was purchased. All software companies now have a shorter turn around time on software development, and if this is also taken into account it might cost the municipality more than it should. If software are kept and not upgraded for a period then money is saved. If the software is eventually replaced with the new computer then the hardware is upgraded and newer software can be kept. The older versions may also be kept in use to ensure uniformity and to save some money. It is not compulsory to upgrade software, nor is it advisable to do so every year or three years. This could ensure larger training bills and more personnel off duty more of the time for this training. Where freeware is used it will amount to less cost and then upgrading regularly may actually bring about change and better productivity.

2.6. As with cars, computers do have moving parts and these parts are negatively affected by dust and smoke particles in the air. The equipment must be serviced at least every three (3) to six (6) months to clear away especially dust and to ensure that the components are not covered by dust which results in heat building up.

2.7. No person should smoke in the server room at all. No food or drink should be allowed in the server room as spillage may damage the equipment. It is also advisable and recommended that no person may smoke near computers as to ensure better protection and also better performance and longer life from the equipment. Since smoke can build up to dust, it is prone to form a layer like dust and cause failure in sophisticated chips. Failure through heat build-up is common with computer equipment.

2.8. The movement of computer equipment must be done with a project plan as this movement usually affects other areas such as IP Addresses and network segments but especially hub population and configuration. In extreme cases such changes also meant a change in router configuration. Such a plan must reach the Head of the Department responsible for Information Technology no later than at least thirty days in advance to ensure proper planning and to properly inform users of such movements and how they will be affected.