EMAKHAZENI LOCAL MUNICIPALITY

NETWORK,PC HARDWARE AND SOFTWARE POLICY

Approval

DOCUMENT:	**NETWORK AND PC HARDWARE AND SOFTWARE**		
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
4th	May 2015	None	E Mnguni 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.

Contents

NETWORK AND PC HARDWARE AND SOFTWARE

PURPOSE OF THE POLICY

The purpose of this policy is to govern the use of the network and computers or devices connected to the network as well as to inform of the legality of actions taken and what are expected of users and support staff.

1. SCOPE AND USAGE OF THE NETWORK

1.1. The network of the Emakhazeni Local Municipality is a government network as the municipality is a tier 3 government institution. The network is to be used for official purposes only and no private work or data or illegal actions, things that are prohibited by national and international laws such as downloading movie files, music or software that is being pirated, is allowed on the network. This includes private downloads of movies, music in any format, software programs including games and other software for personal use and not for official purposes. None of these files may be kept on the network file server for sharing or made available on the network for any reason. Should such files, data or programs, contain any viruses and or backdoors for outsiders to enter the network illegally, all costs incurred to rectify this problem may be recovered from the official responsible for such a breach. Responsibility and accountability for the contravention of international and local laws will be for the municipal manager and mayor if the perpetrator(s) are not known. If the perpetrator(s) are known then they will be held responsible and accountable for all actions taken and can the relevant punishment for the contravention of such a law be made applicable to the person.

1.2. All personal computers (PC's), notebook/laptop computers, workstations, personal digital assistants (PDA's), cellular telephone and any other device not specifically listed here with which one can gain access to the network to store, retrieve or access data or programs at Emakhazeni local Municipality are bound by this policy and the users thereof are bound by what this policy dictates. Not only is the user hereof bound by this policy but also by the National Intelligence laws and amendments there-of, laws prescribing government official's conduct and laws governing the telecommunications and electronic communications of this country as well as international laws where applicable. The network at Emakhazeni forms part of a secure network within the government network where secrets are kept and should be kept to protect the people of this

country against foreign invasions and or terrorism. It is therefore to be kept a secure network without outside network access and all actions on this network should adhere to the National Intelligence Agency laws and amended laws and Regulations.

1.3. The network comprises the physical cabling, points, hubs, routers and file servers as well as the cabinets in which they are kept, i.e. all the hardware. Along with this the network also comprise of all the software installed and used on the network file servers and workstation also called personal computers, notebook/laptop computers and handheld devices mentioned earlier that run software paid for by the municipality and used in the general mandate of the municipality. All physical and virtual connections that are created for the purpose of communication via computer are deemed part of the network.

1.4. This policy includes all persons that are part of the Emakhazeni Local Municipality as permanent employees, contractors or third party suppliers of services and temporary workers of the municipality.

1.5. No computer equipment (hardware) or software may be removed from the site without relevant paperwork and the consent of the supervisor and/or Head of Department to ensure that the equipment and software are generally protected and safe at all times. The equipment may not be removed and used for private or personal use as it is the property of the local municipality and should be used in the service of the local municipality only and not to promote personal agendas.

1.6. No software that is licensed through the Emakhazeni Local Municipality may be installed on any private personal computer (PC), notebook/laptop computer or any other type of computer or device that can use such software and be used to access data and/or the network. All software can be used only for the Emakhazeni local Municipality computers and installed on said computers. These licenses should be kept and controlled by one person that will issue only when software needs to be reinstalled or when a new computer has to be set up. All software used by the municipality must be recorded in a register and must be signed for when it is to be used by a support person for installation. Software may not be taken off the premises without the authorization of the Head of the Department handling the Information Technology for the municipality. All software that must be issued for installation to the support person may only be issued with a reference number of a job card for such

support or software installation. The relevant register must be presented at the annual audit and verified against the job card or copy there-of kept at the office. The register aims to improve control over software and licenses as well as the installation of licensed software on computers. The licenses that have to be controlled are all software that are protected under South African and/or international laws and treaties and that a certain premium has to be paid for. All illegal software must be removed from all official computers as soon as possible to ensure that the legally owned software only is installed on computers.

1.7. The municipality must decide on the route to take about the software to be used. It is either the MS Office suite for which a licensing fee has been paid or the open source applications such as the Open Office suite that is freeware. Freeware may be installed on other computers without further control over it but all licensed software has to be controlled and properly protected against software piracy. All unused and illegal software programs must be removed from the computers where it is installed in order to comply with the laws and the relevant license agreements.

2. NETWORK ACCESS

2.1. All users of the network at Emakhazeni Local Municipality must be registered users on the network and must be created as users of this network on the file server in either directory services or just the file server with a valid username and password. This will ensure control and effective problem resolution at all times. All users must have an allocated space on the file server where data can be saved individually or collectively as a group of users working on one project such as Engineering. Only such data will be backed up regularly. This will also provide users with access to the network services available on the network.

2.2. The minimum user rights must be applicable in all instances when users are created since it can create a security breach on the network. Users should only have Administrator or equivalent rights on the server when they work on their own user directories or folders. The norm and default creation of a user is to be created with full control and access rights to the server. This can enable users to manipulate data and applications and can result in the corruption of data and or applications resulting in huge support and repair bills. The minimum rights assigned to all users will be Read rights and to Browse the network. Extra rights and privileges must be assigned only on request

and where it is in the interest and explicitly necessary to have such rights. No user should be allowed to have control over the network or file server(s) at the office unless such a person was employed for that specific task. This will ensure better control and make sure that the malicious intent is reduced.

2.3. Each computer has to have a marked network point in the office where the computer equipment is installed giving access physically to the network and network services available.

2.4. Physical access to the network server room and file servers is prohibited for all users except relevant support (ICT) personnel appointed in writing. In the absence of such person or personnel a delegate should be appointed to perform minimum functions as and when required. This person should preferably be a computer support person or have relevant knowledge to perform such tasks, even on file servers as and when required.

2.5. Access to the network is guaranteed and available during all office hours from 07:30 to 16:00 daily. The network must be accessible from 06:00 to at least 18:00 daily. Any deviation to this must be discussed with the relevant Head of the Department responsible for Information Communication Technology and authorization must be obtained for such a deviation. Access to the network after hours should as far as possible be restricted and where possible totally avoided. Exception is the access to the users mail on a secure access (*https:*). This is for the sake of safety and network backups. Should files be open during backups it will not be backed up and data loss may occur.

2.6. All users must use a password with their usernames or user ID's to access the network. The password should consist of no less than six (6) characters without repeating such characters more than three (3) times. The password can be made up of any combination of letters and numbers. Passwords should also expire every thirty (30) days and old passwords may not be used for at least six (6) months.

2.7. A properly implemented directory service should be implemented on the network to ensure better security and safety of data and information. The directory should provide access to relevant network services and exercise control over such services.

2.8. All users must be granted at least one (1) network connection and not more than that. If more than one connection is allowed for a user to the network then it could mean

defeating the security system. This will allow network user names to be shared and even logged in more than once, exploiting the network and services without being able to pinpoint the guilty party.

2.9. No user may use the network username of the network support person or of another user with more rights than himself or herself. Where it is found that a user needs more rights he/she must apply for this from the Head of the Department responsible for Information Communication Technology.

2.10. No user may use the Administrator or Admin user accounts or ID's to access the network. These accounts should be reserved for network administrators only and should also be controlled. The password of this account should be changed at least every thirty (30) days. The password should be kept in an envelope with the Head of the Department responsible for Information Technology. This account should only be used when necessary repairs are undertaken on the network and also when new implementations are to be done and the Administrator or Admin user account is necessary.

2.11. When a user leaves the employ of the municipality his/her user account must be locked on the last day of work. All official files or documents that user is the owner of must be copied to a location where it can be used and or updated. The relevant user account should then be deleted along with the user directory allocated to that user on the network file server.

2.12. When a user account is not accessed for a period of three (3) months that user account should be locked. When the user account is not used at all it should be deleted from the network and all files saved to a location where relevant personnel can access it.

2.13. All users should ensure that when they leave their workstations they log out from the network, especially if they will be leaving the workstation unattended for longer than ten (10) minutes. Especially where they access transversal systems or financial applications such as the Munsoft program. It is important to remember a malicious person to gain access to the network may use an unattended logged on workstation. Even visitors may cause irreparable damage to the network or a financial system or may access information that is conf identical. All data on the network should however be considered as

confidential, especially when visitors are visiting the office for any reason.

2.14. No person other than the person the computer was issued to may use it. Officials may allow access to another official for purposes like accessing and verifying programs and data. Private persons may under no circumstances be allowed to use any computer or the computer network. Irrespective of the age and qualification of the person he/she may not access or use the computer.

2.15. All users will receive an Internet Protocol Address (IP Address) with which he or she can access the network and Internet. This IP Address is assigned permanently to the relevant user by assigning it to the relevant network card. This will ensure that the user has the relevant access he/she needs. When a network card becomes faulty care should be taken that the new network card should use the same IP Address. The faulty network card can then be sold or thrown away. Important to note is that there are companies and individuals that collect such cards and recycle it. This option can be explored to generate a revenue and use the funds where needed.

2.16. Users that will be away from work for long periods of time should inform the network support person to lock the user account so no one can gain access using that user account. This will ensure better security on the network and safety of all data on the file servers. The user can then request for unlocking the user account when returning to the office.

2.17. Where the municipality needs access to transversal systems at provincial and national levels provision should be made for this to occur effortlessly and security procedures are in place to ensure safety of data and applications. Only people that are registered and specifically granted access to such systems must be allowed to have the relevant software on their workstations/computers. The user account information and passwords should not be shared at all with any other member of the municipality y regardless of rank, stature or designation. The person should not be hassled in any way to give such information as that person has undergone security checks where applicable and changes are registered on the system(s) against the user ID or account and the user will be held responsible for changes implemented on the system(s).

3. NETWORK SERVICES

3.1. Network services include all relevant and applicable applications that ensure the use and not abuse of the network. File services and printing services will be provided on the network as well as a backup service for official data and documents only. The saving of private data, applications and documents on the file server is strictly forbidden and will be removed without notification to the relevant owner. Although the individual has a right of privacy the file server is a public entity and environment that has to be respected and will only be used for saving official data and documentation. All documents saved on a file server, whether in a user allocated space or not will be deemed public property and can and will be removed from the server without notification to the owner of the file. There will be no privacy statements and/or claims of files saved on the file server.

3.2. Printing services are there for the explicit use of the municipality in the execution of the duties there-of according to the relevant laws and regulations. Private printing and printing of private and personal files, documents or data are prohibited and can lead to disciplinary action with regards to the abuse of government property and/or illegal contravention of network and government security. All users may use appointed printers and printer devices such as photocopiers that can perform the functions of a network printer. Printers to which restrictions have been added are deemed off limits to all except the persons appointed as users of that particular printer and/or printer device. One such occurrence may be printing to the colour laser printer.

3.3. Only relevant network services and clients must be run on the government networks and installation of other services and clients are prohibited. This may allow the network to become insecure and unstable and cause downtime.

3.4. All users on the network will receive a specified amount of space on the network file server where data may be stored. Such folders or directories are subject to regular audits and investigations and should contain only official data or work related information. All private and/or personal data with the exception of curriculum vitae (CV) are prohibited on the server.

3.5. The directory services implemented should ensure control and ensure that all relevant information is safe on the network. It should also be monitored regularly to ensure that there is no

abuse of services or devices. Where abuse is found it should be properly investigated and acted against to ensure the municipality is not exploited or exposed as an organization abusing public funds.

3.6. Network expansion should be allowed to allow for handheld devices to connect to the network. Such devices must adhere to all the security measures employed at the municipality.

3.7. The network provides every user with a valid Internet Protocol Address (IP Address). This address is sometimes linked to certain services and access options and should not be swapped out between users. Such addresses can be assigned dynamically via DHCP server or statically assigned on the workstation itself. Users should not use each other's IP Addresses to gain access to certain services but should apply for access to such needed services via memorandum to the Head of the Department responsible for Information Technology.

4. NETWORK AND PC SUPPORT

4.1. The appointed network support personnel should undertake all network support only and no user may interfere in such actions unless appointed to do so in writing by the Head of the Department responsible for Information Communication Technology. This is to ensure that where support contracts are running and paid for the municipality gets the relevant service from the provider. The service provider may refuse such work when there is interference from the client and this may cause disruption on the network. When a support company is used there should be one person appointed to liaise with the company from the municipality and all actions should then flow via this person. This is to ensure responsibility and accountability for work done on the network. Where a person of the municipality becomes skilled in an area that could assist the provider he/she may be approached via the liaising person for such information to assist when such skills are not readily available. Care should be taken that the support provider does have the necessary skills or access thereto to perform all necessary duties in this regard. The support provider may escalate problems but care should be taken that trustworthy people are used and not potential network threats. If the municipality makes use of employed personnel the municipality must ensure that the relevant helpdesk and call support structures are in place. Care should be taken that a call that cannot be resolved locally be escalated to properly trained and trusted

personnel and not to people that are known to exploit such instances.

4.2. All support must be performed against a logged call with the detail of the call that was logged. Such a call should then be attended to as per request and written off after resolution of the fault. A copy of the job card should be kept with the liaising personnel member to ensure that the work was performed to standard and satisfaction.

4.3. All network support should be given priorities and should be attended to immediately. All calls where all users are affected should be attended to immediately. A list with the priority work should be drawn up and attended in that order when it occurs.

4.4. It is the responsibility of the computer user to log any faults with the computer or the network that he/she may experience. Faults that are not logged will not be attended to and the network support personnel or service provider cannot be held responsible for such faults or problems. Faults mentioned to the support person verbally cannot be seen as an official logged call and a fault has to be logged irrespective of the response from the network support person or company. Faults attended to without a job card and official fault log can be deemed as free of charge and may not be paid for. The support person or provider should therefore ensure that all work he/she does are properly logged and documented.

4.5. No user, irrespective of his rank or stature are allowed to approach the support person directly when faults are logged through a helpdesk to ensure that favours are not part of the operation. As stated above only work that is logged will be and should be paid for. No person may under any circumstances make use of the support person or provider company to repair privately owned personal computers during official times and have such bill be sent to the municipality. The only exception is where this was agreed to in the person's contract and this would be part of the person's benefits. All privately owned personal computers or devices are to be repaired outside of the contract with the municipality and would be for the account of the relevant person. Should a company be used and they decide to provide a support person for private repairs as needed this must be done then outside of the agreement with the municipality and are for the account of the person himself/herself. A separate person and not the person allocated to perform the support duties for the municipality on the day should also do this. Where the municipality employs a

person that person are not allowed to perform any private duties within official working hours, irrespective of the requester. That will include all members of the executive committee, councilors, the mayor or any other person that forms part of the municipality. Such a person may also not bring in private work to be performed during official working hours. Such actions will be seen as a contravention of the agreement or service contract.

4.6. The municipality has to support or provide for support on all the local area networks (LAN) it has and that are part of the municipality. All Wide Area Network (WAN) connections are the responsibility of the relevant service provider like SITA for one or a private service provider that an official agreement has been entered into.

4.7. Only recognized and appointed support technicians are allowed to work on computers of the Emakhazeni local Municipality. No other person, regardless of connection, stature, rank or qualification may work on any computer or computer equipment belonging to the Emakhazeni local Municipality unless the problem was escalated to the person by either the support person or the Head of the Department responsible for Information Technology in writing and the escalation was favorably accepted.

4.8. Only work directly requested from the support person or company will be performed and no extra work may be done at all. For instance when both a software problem is experienced and a hardware problem both should be listed and reported. If this is not done, only the reported problem or fault will be dealt with. If no job card exists for a fault experienced such a fault must first be logged before it is being attended to. This has to be done in order to assist in the recordkeeping of expenditure on computers and related equipment. No support task may be undertaken without such a job card.

5. NETWORK AND PC HARDWARE

5.1. As stated above all computer equipment that forms part of the network or that are used on the Emakhazeni Local Municipality and that was paid for or donated to the municipality are the property of the local municipality. The equipment is there to provide certain services to the users on the network and to enhance the service of the municipality to the community.

5.2. None of the mentioned items may be removed individually or in-group from the site without the explicit consent of the Head of the Department responsible for Information Communication Technology. All network equipment is to remain on site unless the Head of the Department responsible for Information Communication Technology authorize such a move when necessary for repairs, replacement and/or reconfiguration. All other equipment may be removed with the consent of a delegated person but network equipment will not be part of this. If it is an emergency another Head of Department that is taking care of the duties in the absence of the appointed member should give authorization. This is done to protect the network and services as well as data on all file servers.

5.3. Under no circumstances may any person use any file server as a workstation to perform his/her duties. The server is and should be a dedicated server and network service provider to clients on the network. Its resources and processes should not be hogged by desktop applications run on the network file server.

5.4. No user irrespective the rank or stature is allowed to remove network cables from the network or server or even computer for use elsewhere. This can be seen as sabotage or theft to disrupt network services and are subject to disciplinary action against such a person. Theft will be subject to the relevant laws of the country for which jail terms may be applicable.

5.5. All computer and network hardware must be subjected to a service every six (6) months and a certificate must be issued that shows that all fans are working properly, are clean and excessive dust have been cleared away. It should also involve the hard disks and any other component of any network device and computer. This is done to lengthen the life of equipment and ensure that problems are minimized.

5.6. All computer equipment that are broken or fail as a result of rough handling and/or abuse can be recovered from the relevant person guilty of such an offence. Care should be taken in such proceedings that all relevant avenues have been explored to educate and train the person as to ensure that the safety of the equipment is priority. Unnecessary rough handling is something that has to be checked into and abuse and abusive actions should be sternly reprimanded. If the user persist with this action the relevant steps should be taken immediately and such equipment should be taken away from that person, irrespective of his/her duties.

5.7. Theft of equipment should be reported to the relevant authorities and should be dealt with. Care should also be taken that security measures in place are adequate and that measures implemented are cost effective and efficient.

5.8. Where computer equipment have to be moved from one location to another the relevant information should be given to the support person involved at least fourteen (14) days beforehand. This is to plan for any contingencies such as movement or installation of cables and also expansion of existing equipment. This can also provide time to acquire new equipment should this be necessary or the relocation of current equipment and the reconfiguration there-of. Reconfiguration of equipment is very important as to ensure that when the actual move takes place the items can be plugged in and will work without major disruptions in work.

5.9. Support personnel should be consulted on the purchase of new hardware to ensure that the new hardware can work with current hardware and also the network and network software and that the new hardware will not cause downtime on the network.

6. NETWORK AND PC SOFTWARE

6.1. All network and personal computer software installed on the file servers and personal computers acting as workstations on the network are deemed licensed and the property of the Emakhazeni local Municipality. All privately owned software must be removed from such computers and file servers regardless of the use there-of. The Public Administrations Committee issued instructions that only official software is allowed to be on any government computer, regardless of the use there-of. Since this is, also a government office such instructions must be adhered to in order to avoid further steps taken.

6.2. All computer software that are licensed and used at the local municipality must be listed in a register and properly issued to a user. Licenses that are left over afterwards should be declared and not issued for private use or privately owned computers unless specific provision was made for such installation in a government law on national level. No local government laws may dictate such steps; as such registers must be subjected to national Treasury inquiries and inspections as well as that of the Auditor General. Failure to submit such registers may result in penalties and/or subpoena to give evidence before the Public Accounts Committee.

6.3. Only relevant, official software may be used and installed on computers. No games or any type of gaming software or activity pack or entertainment software may be installed on official computers. This instruction was given under Public Administrations Committee as to ensure improvement of work performance and better utilisation of especially computer equipment. That entails that even games that comes with the operating system are not allowed to be installed for any purpose. Training computers may have such software installed for reference and specific training only. Common complaints from public were that government officials spend more time playing computer games than attending to the needs of the public and the community as a whole. Regardless of whether the executive committee allows games on computers or not this statement should be taken into consideration as it reflects negatively on public officials and government as a whole.

6.4. Management software may be installed and implemented on the network and all connected computers to ensure better control and management and administration of the computers. Audits may be done from time to time and should it be found that illegal software are installed on such a computer it will be removed without prior notification. The law states that each person should have the right to privacy but a government network and computer is a security area that no personal or private information may be kept for any purpose.

6.5. All software that are planned to be installed or upgraded on the network must be communicated at least fourteen (14) days in advance to the Head of the Department responsible for Information Communication Technology. A proper project plan must be submitted as well as all downtime planned and the affected workstations of the municipality as well as how they will be affected. This will ensure timeous notification and planning can be done to overcome negative affects of downtime. This will also ensure that there is a continuation of services regardless of the downtime.

6.6. It is not recommended to install and configure themes of any type on computers as it does have a negative affect on the performance of both the computer and the network as a whole. Computers and software should be kept standard as far as possible or display only screensavers that will enhance the municipality's image. Desktop themes that slow performance must be removed as it will lead to requests for faster computers and can result in unplanned expenditures. It is known that government officials elsewhere have in the past installed such themes and

software to show the inadequacies and lack of performance of computers purely to receive newer computers.

6.7. No BIOS or screensaver passwords are allowed on computers of the municipality unless it is stated that the relevant computer is a security risk and has to be protected. Such passwords should then be made available to the relevant Head of the department or office manager and used only in the absence of the relevant user if data is needed urgently from that computer.

6.8. The support personnel should be consulted before new software is purchased as system requirements should be adhered to and also network standards should be considered. In some cases newer software cannot work with already installed software off the shelf and relevant patches should be downloaded or obtained before such software is installed and implemented. Consulting the support staff will ensure that the matter is investigated and that all considerations are taken into account to lessen the downtime and ensure that there is no extra software and hardware needed for the software to work properly. The support personnel should also ensure that the network would not be negatively affected by the planned software's installation and usage.