05	ANTI-VIRUS AND FIREWALL USAGE AND APPLICATIONS	
*	computers (to read)	computers and mobile devices
1.1	The municipality should have in place an anti-virus strategy that will protect or aim to protect all computers on the network or connected to the network either via cable media or through wireless connections. All computers should have anti-virus applications installed to guard against the threat of computer viruses. The strategy should include not only the file server but also all computers that connect to the network at the Emakhazeni Local Municipality.	The municipality should have in place an anti-virus strategy that will protect or aim to protect all computers on the network or connected to the network either via cable media or through wireless connections. All computers and mobile devices should have anti-virus as defined by the ICT administrator and the user is not authorised to change the application without permission. Applications are installed to guard against the threat of computer viruses. The strategy should include not only the file server but also all desktop computers , laptops and tablets / smart phones that connect to the network at the Emakhazeni Local Municipality.
1.3	All computers that connect to the Emakhazeni local Municipality network should be protected against viruses	All computers and mobile devices that connect to the Emakhazeni local Municipality network should be protected against viruses .....
1.4	All e-mail that is received should be scanned for both spam mail and virus threats received via e-mail. This can be done at both the server and the workstation and should be used to ensure added protection of the network and the computers on the network.	All e-mail that is received should be scanned for both spam mail and virus threats received via e-mail. This can be done at both the server and the workstation and should be used to ensure added protection of the network and the computers and mobile devices on the network.
1.5	Along with a recognised anti-virus application for the server and workstations there should also be a recognised firewall built into the system or installed as third party software. It should be noted as described above that Windows Internet Information Server is not considered a secure environment and firewalls should be properly configured to protect such services running. Where possible Internet Information Server should not be	Along with a recognised anti-virus application for the server and workstations there should also be a recognised firewall built into the system or installed as third party software. It should be noted an independent Server is considered to secure the environment with firewalls to be properly configured to protect such services running. Internet Information Server should not be used as a web server that is connected to a secure network. No instances have been found where such servers have not been successfully penetrated by hackers' and data exposed to the world or corrupted. Since this is a government network and a security

	used as a web server that is connected to a secure network. No instances have been found where such servers have not been successfully penetrated by crackers and data exposed to the world or corrupted. Since this is a government network and a security environment, it should therefore be protected by a reputable firewall famous for stopping threats to any network.	environment, it should therefore be protected by a reputable firewall famous for stopping threats to any network.
1.6	Firewall software should be installed on all computers and mobile devices accessing the Internet or a similar remote network such as a bank's secure site where access to the site is not gained through the Internet connection hosted by the file server. In such cases, a dedicated link is made to the outside world and no protection is gained when a firewall is setup only on the file server. In such cases the computer does not make use of the file server at all and the data transmission is therefore not always safe. Although precautions may have been taken at the bank it might not be enough and access may be gained to the network via the computer connecting to the remote network.	A reputable anti-virus and firewall software should be installed on all computers and mobile devices accessing the Internet or a similar remote network such as a bank's secure site where access to the site is not gained through the Internet connection hosted by the file server. In such cases, a dedicated link is made to the outside world and no protection is gained when a firewall is setup only on the file server. In such cases the computer does not make use of the file server at all and the data transmission is therefore not always safe. Although precautions may have been taken at the bank it might not be enough and access may be gained to the network via the computer connecting to the remote network.
01	MANAGEMENT OF ICT PERSONNEL	
	Cracker (replaced with)	Hacker
	Cracker Usually malicious person who access a network illegally. He/she usually breaks down the network and places viruses to cover his/her tracks and to ensure downtime on the network.	**Hacker** A person who circumvents security and breaks into a network, computer, file, etc., usually with malicious intent. He/she usually breaks down the network and places viruses to cover his/her tracks and to ensure downtime on the network.

02	NETWORK AND PC HARDWARE AND SOFTWARE	
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.	The network of the Emakhazeni Local Municipality (category B) 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.
03	ELM - INTERNET POLICY	
	Users with Internet access may not have any or all of the following applications installed on their workstations/computers as it abuse available bandwidth and can be used to defeat security systems and software in place: • MIRC • ICQ	Users with Internet access may not have any unauthorised programmes or material loaded on their PC/laptop for private or that is not approved by ICT manager. Any other IRC-related application not mentioned here, except that which may be allowed by management that will be part of

	- Yahoo! Buddy/Companion - MSN Messenger - AOL Companion - BonziBuddy Any other IRC-related application not mentioned here, except that which may be allowed by management that will be part of communication packages in place on the network such as a relay agent shipping with programs such as GroupWise, MS Outlook and MS Exchange. Such programs are guaranteed as secure communications by their owners and will not aim to defeat the security systems and software installed and implemented on the network. The mentioned applications have been found to carry intruders successfully into secure environments and can disrupt network operations and cause downtime or add to the distribution of computer viruses.	communication packages in place on the network such as a relay agent shipping with programs such as GroupWise, MS Outlook and MS Exchange. Such programs are guaranteed as secure communications by their owners and will not aim to defeat the security systems and software installed and implemented on the network. The mentioned applications have been found to carry intruders successfully into secure environments and can disrupt network operations and cause downtime or add to the distribution of computer viruses.
04	ELM-EMAIL POLICY	
	No Changes	
05	ELM Anti Virus Policy	
	No Changes	
06	ELM-DATA MANAGEMENT	
	No Change	
07	ELM_Servers_Security_Policy	
7	The server security policy is applicable to the server room, to server equipment owned and/or operated by the Emakhazeni Local Municipality, or Disaster Management Center of the Dr Kenneth Kaunda District Local Municipality, external service providers and any servers outside the building belonging to the municipality used for purpose of providing ICT services and are on the network infrastructure of the	The server security policy is applicable to the server room, to server equipment owned and/or operated by Emakhazeni Local Municipality, external service providers and any servers outside the building belonging to the municipality used for purpose of providing ICT services and are on the network infrastructure of the Municipality.

	Municipality.	
08	ELM-ASSET M ANAGEMENT POLICY	
	No Changes	
09	ELM-SYSTEM DEVELOPMENT LIFE CYCLE	
1.3	A project plan with cost and time frames must be compiled and submitted to the IT Committee and Executive Committees for such a project, if it is decided upon. It is advisable that all member local municipalities tackle such a project collectively and not individually to save costs and ensure that the product is well utilized.	A project plan with cost and time frames must be compiled and submitted to the ICT Steering Committee and Executive Committees for such a project, if it is decided upon. It is advisable that all member local municipalities tackle such a project collectively and not individually to save costs and ensure that the product is well utilized.
10	BACK-UP MANAGEMENT POLICY	
9.1	Only the following member(s) of staff are authorised to load software onto any part of the network: (names) according to the software installation policy.	Only ICT staff are authorised to load software onto any part of the network: according to the software installation policy.
9.3	Niall Carroll who is the DMICT will ensure that all staff is aware of this by both signing of the policy, induction, workshop, etc	The DMICT will ensure that all staff is aware of this by both signing of the policy, induction, workshop, etc
11	11.1 Provide the statutory and regulatory framework for the policy. To comply with all relevant legislative requirements including: 11.2 The Constitution of the Republic of South Africa, 1996 11.3 Municipal Structures Act, 1998 11.4 Municipal Systems Act No 32 of 2000 11.5 The Municipal Supply Chain 11.6 Management Regulations 11.6 Division of revenue act 11.7 Municipal Finance Management Act No 56 of 2003 (MFMA)	11.8 mSCOA

11	ELM Web Content Management Policy	
	No Change	
12	USERNAMES AND PASSWORDS	
1.6	All users must use a password to access the network and users should be forced to change all passwords every sixty (60) days. This will ensure a better measure of control against illegal outside attacks and provide a more secure environment. Apart from forced changes, no password may be used concurrently and unique passwords must be chosen. Passwords should not be repeated for at least six (6) months or cycles of password changes.	All users must use a password to access the network and users should be forced to change all passwords every thirty (30) days. This will ensure a better measure of control against illegal outside attacks and provide a more secure environment. Apart from forced changes, no password may be used concurrently and unique passwords must be chosen. Passwords should not be repeated for at least six (6) months or cycles of password changes.
13	ICT Change Management and Control Policy	
	No Changes	