EMAKHAZENI LOCAL MUNICIPALITY

ANTI-VIRUS PROCESS POLICY

Approval

<table>
<tr><td>DOCUMENT:</td><td colspan="3">Guidelines on the Anti-Virus Process</td></tr>
<tr><td>Copy Number:</td><td colspan="3">Master Copy</td></tr>
<tr><td>Compiled by:</td><td>Niall Carroll</td><td>Reviewed by:</td><td></td></tr>
<tr><td>Compilation Date:</td><td>August 3003</td><td>Review Date:</td><td></td></tr>
<tr><td>Version:</td><td>V 1.2</td><td>Revision:</td><td></td></tr>
<tr><td>Distribution:</td><td>All</td><td>Classification:</td><td></td></tr>
<tr><td colspan="2">Document Release Approval</td><td colspan="2">Document Acceptance</td></tr>
<tr><td rowspan="2">Releasing Authority:
Director: Cooperate Services</td><td>ICT Division</td><td rowspan="2">Acceptance Authority:</td><td>Council</td></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td>Date Released:</td><td>Date Accepted:</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>Signature:</td><td>Signature:</td></tr>
</table>

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

ANTI-VIRUS AND FIREWALL POLICY

PURPOSE OF THE POLICY

The purpose of this policy is to ensure the protection of all computers and mobile devices and data on the network by implementing steps that are precautionary and not remedial. This includes computers and mobile devices making outside connections through secure channels and not through the file server.

1. ANTI-VIRUS AND FIREWALL USAGE AND APPLICATIONS

1.1. The municipality should have in place an anti-virus strategy that will protect or aim to protect all computers and mobile devices 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 applications installed to guard against the threat of computer viruses. The strategy should include not only the file server but also all computers and mobile devices that connect to the network at the Emakhazeni Local Municipality.

1.2. The software should be configured to monitor new connections and to immediately install a version of the software decided upon to be used for protecting the network. The installation should be done before access is granted to network services, therefore during the start-up and logon procedures. It should also then upgrade the anti-virus pattern files and scan engine to be the latest versions available.

1.3. All computers and mobile devices that connect to the Emakhazeni local Municipality network should be protected against viruses and therefore regular updates should be made available and done on all computers and mobile devices at least once per week. This will ensure that the network is at all times operational where possible. It is impossible to guard against all computer viruses and when a virus threat is detected and the scope of the problem is too much for one person to handle he/she should be allowed to escalate the problem to contain the virus as quickly as possible. The quicker the response the more likely it will be that data corruption is limited and data protected against outside exposure and exploitation.

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 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 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.

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.

1.7. All users should take care that although there might be good data recovery strategies available it does not guarantee that data corrupted by a computer virus will be recovered and restored. The support personnel or company can therefore not be held responsible for data that are lost due to computer viruses on the network or the distribution there-off by users. Support personnel can also not be held responsible for viruses that infect the network, bypassing anti-virus scanners in the process since viruses are developed nowadays to render anti-virus applications useless.

1.8. All firewalls and anti-virus applications should run on start-up, in other words while the computer is loading relevant files to render it operational and ready for input from the user of the computer. These software applications should not be unloaded or disabled unless specifically instructed by the support person.