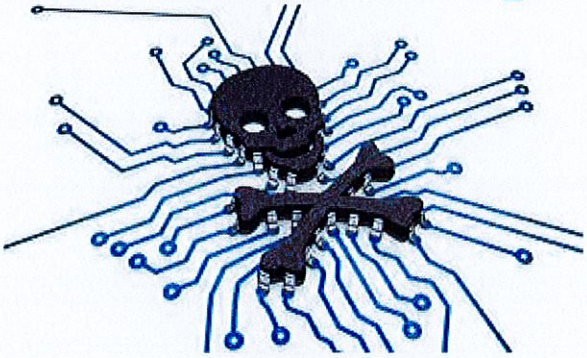
Thulamela Municipality



ANTI-VIRUS POLICY

DATE	1 July 2022
REVISION	0.2
Document ID	ICT-017-7718

Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, CDs and Memory sticks. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Thulamela Municipality in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of Thulamela Municipality is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by Thulamela Municipality employees to help achieve effective virus detection and prevention.

Scope

This policy applies to all computers that are connected to the Thulamela Municipality network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both Municipal-owned computers and personally owned computers attached to the Thulamela Municipality network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, servers and cloud storage connected to the network.

General Policy

1. Currently, Thulamela Municipality has a Microsoft Endpoint Protector Antivirus licensed through System Centre. Licensed copies of Microsoft Endpoint Protector Antivirus can be obtained within a domain automatically when a user connect a device to the Municipal network. The most current available version of the anti-virus software package will be taken as the default standard. Where for any reason the Microsoft Endpoint Protector Antivirus is not available, an open source antivirus will be provided temporarily.

2. All computers attached to the Thulamela Municipality network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

3. Any activities with the intention to create and/or distribute malicious programs onto the Thulamela Municipality network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

4. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the ICT Section immediately at 7684 / 7656 / 7678. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

5. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the ICT Section.

6. Any virus-infected computer will be removed from the network until it is verified as virus-free.

TAM MT

Rules for Virus Prevention

1. Always run the standard anti-virus software provided by Thulamela Municipality.

2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

3. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.

4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

5. Files with the following filename extensions are blocked by the e-mail system: .exe, .zip, related. While sending/receiving business-critical files with banned extensions, such as use of a file compression utility please be advised that most of those extensions are also blocked on the email services, so even if you have compressed your own file into a Zip file it may not reach its destination as the email service may block it.

6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

7. Avoid direct disk sharing with read/write access. Always scan a memory stick for viruses before using it.

8. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

9. Back up critical data and systems configurations on a regular basis and store backups in a safe place.

10. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

ICT Section Responsibilities

The following activities are the responsibility of the Thulamela Municipality's ICT Section:

11. The ICT Section is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted to the workstation directly from the domain distribution server known as WSUS. System Administrator needs to check antivirus updates regularly for updated information or definitions.

12. The ICT Section will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.

13. The ICT Section will apply any updates to the services it provides that are required to defend against threats from viruses.

14. The ICT Section will install anti-virus software on all Thulamela Municipality owned and installed desktop workstations, laptops, and servers.

15. The ICT Section will assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes. The ICT Section will only advise or and provide open source anti-virus software in these cases.

TAN MT