Anti-Virus Policy

Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event and will spread from one computer to another. Viruses can be transmitted via e-mail, downloadable Internet files and removable media (flash drives, etc). Viruses can be referred to as malware, adware, and spyware programs. 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 the City of Milwaukee in terms of lost data, lost staff productivity, and/or lost reputation.
As a result, one of the goals of the City 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 City employees to help achieve effective virus detection and prevention.

Scope

This policy applies to all computers that are connected to the City network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both city-owned computers and personally-owned computers attached to the network. The definition of computers includes desktop workstations, laptop computers, servers and other devices connected to the city network.

General Policy

1. Currently, City departments have various anti-virus software such as Trend Micro, McAfee, Norton and Microsoft Essentials. Complete and current anti-virus applications (including version numbers) can be found at: http://www.milwaukee.gov/antiviruslist

2. All computers attached to the city 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 City 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 department IT staff or the Information and Technology Management Division immediately by calling 286-2777. 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 IT department.

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

Rules for Virus Prevention

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

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 co-worker) 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, .bat

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

7. Avoid direct portable drive (e.g. memory stick) sharing with read/write access. Always scan a portable drive 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. IT staff should 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.

IT Department Responsibilities

Given the distributed nature of IT in the City the responsible parties vary depending on the department. If a department does not have IT staff, the IT Department is defined as the Information and Technology Management Division (ITMD). The following activities are the responsibility of the City IT staff:

1. The IT staff is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted on MINT. Check MINT regularly for updated information.

2. The IT staff will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.

3. The IT staff will apply any updates to the services it provides that are required to defend against threats from viruses.

4. The IT staff will install anti-virus software on all City owned and installed desktop workstations, laptops, and servers. If this is not applicable for some equipment a notice should be sent via email to the Chief Information Officer for exclusion to this policy.

5. The IT staff will assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes. The IT staff does not provide anti-virus software in these cases but it is required to be installed if the employee wishes to use a personal device.

6. The IT staff will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT staff may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

7. The IT department will perform regular anti-virus sweeps of files.

8. The IT department will attempt to notify users of City systems of any credible virus threats. Note: the IT department will never ask via e-mail for a user to click on a link – this is a common phishing method. If necessary the IT department will communicate via email or telephone messages. Virus reports will not be acted upon until validated. Departmental employees should not forward these or any virus warning messages unless specifically directed to by the ITMD staff.

Department and Individual Responsibilities

The following activities are the responsibility of City departments and employees:
1. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.

2. Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

3. All employees are responsible for taking reasonable measures to protect against virus infection. Save all work (documents, spreadsheets, drawings, etc) on network drives or infected computers will mean a loss of data.

4. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the City network without the express consent of the IT department.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.