

**Office of the Chief Information Officer
Enterprise Policy**

Policy Number: CIO-073

Effective Date: 06/01/2002

Revision Date: 08/22/2008

Subject: Anti-Virus Policy

Policy: This policy supports the Enterprise Architecture for security and outlines procedures that must be followed to protect the Commonwealth. The purpose of this policy is to help protect all computing devices from malicious software (viruses, trojans, worms, hoaxes). Malicious software hereinafter will be referred to as viruses. Enforcement of the anti-virus policy must be verified on a regular basis and documentation of agency action should be available for review.

Responsibility for Compliance:

Cabinet Responsibilities:

Agency CIOs are responsible for designating a cabinet technical contact for virus-related issues. These contacts have access to McAfee's technical support for problems that cannot be addressed by them and/or COT. The contacts are listed on the state's anti-virus website at <http://technology.ky.gov/security/default.htm>.

The systems administration staff that is responsible for supporting the agency is also responsible for ensuring that the appropriate virus protection software has been installed and is functioning properly on all computing equipment. COT recommends that agencies make use of McAfee ePolicy Orchestrator to assist in updating and maintaining antivirus software installations and enforcing antivirus policies.

Cabinets are responsible for their agencies' compliance to the Anti-Virus Policy, as well as all enterprise policies. Failure to police their agencies could result in a loss of networking services for offending agencies.

COT Responsibilities:

COT administers the enterprise agreement for virus protection software that exists between the Commonwealth of Kentucky and McAfee, Inc. More detailed information concerning the enterprise agreement and purchasing McAfee software can be found on COT's antivirus website at http://technology.ky.gov/security/mcafee_info.htm. The McAfee Enterprise licensing participants are able to download anti-virus software from the McAfee website by entering a grant number which will be given to participants when they purchase licenses from the enterprise agreement.

COT maintains an ftp site, <ftp://sunset.state.ky.us/pub/virus>, which allows McAfee Enterprise licensing participants to quickly and reliably update and upgrade workstations and servers. The most current DAT files will be made available at the root of this site for updates as soon as McAfee releases them.

As content of the anti-virus ftp site changes and/or other pertinent anti-virus-related information becomes available, a member of COT's Virus Defense Team will send a message to McAfee Enterprise licensing participants.

Policy/Procedure Maintenance Responsibility: This Enterprise Policy has been approved by the Enterprise Architecture and Standards Committee and constitutes an element of the Security Domain in the Enterprise Architecture. The Commonwealth Office of Technology, Security Administration Branch is responsible for maintaining and updating this policy. The revision review cycle for this policy is annually.

Enterprise Standard: All computing devices must be scanned for viruses. McAfee virus software products are the enterprise standards for virus scanning. If a home computer is used to access state resources, agencies and employees must ensure that computers connecting to the state network meet the same standards as computers in the workplace. Agencies that have purchased McAfee licenses for workplace computing devices have the option of purchasing the Home Use Option which allows McAfee to be installed on Home computing devices. If a business case exception has been approved for other anti-virus scanning software, the following procedures still apply.

Procedures: All state agency employees, contractors and/or third parties accessing the Commonwealth of Kentucky computing environment must avoid situations, which increase the risk for infection by viruses. All files must be scanned prior to execution or use. Reasonable precautions must be taken to prevent the possibility of virus infection.

Only approved software is allowed to reside on Commonwealth of Kentucky owned computer resources, unless otherwise approved by the employee's supervisor, proof of ownership/origin can be demonstrated, and such use does not violate any copyright. Authorized individuals such as systems administrators should install such software. This practice will help minimize the risk of a virus or other malicious software being introduced into the Commonwealth of Kentucky computing environment.

The following steps are required:

- Step 1. All files, including externally supplied CD's and other media, must be checked for viruses when loaded on any computing device. This can be accomplished by the use of the latest release of McAfee's virus protection software, which is the Commonwealth's enterprise IT standard software for virus scanning.
- Step 2. Workstation and server settings must be set to scan all files, preferably both inbound and outbound files, with full logging enabled. However, as a minimum, all inbound files must be scanned. Workstation "on-access scanner" must be set to scan all files. E-mail scans must be set to scan all attachments and compressed files. Download scans must be set to scan all files, and the Internet filter shall be enabled. Exclusions shall be implemented on a case-by-case basis. Server "on-access scanners" must be set as a minimum to scan program files with suggested file extensions, which are posted on the state's anti-virus website at http://technology.ky.gov/security/mcafee_info.htm.
- Step 3. Routine full scans of all files on servers and workstations shall be scheduled regularly, at least weekly. Routine DAT updates engine/software upgrades, shall be scheduled regularly, at least daily.
- Step 4. Backups of critical data continue to be a necessary part of an effective defense against computer viruses. Agency disaster recovery plans shall work hand in hand with anti-virus procedures. It is important to note and plan for the fact that backup files may also be infected.

In addition, systems administration staff shall alert users of other precautions to avoid viruses, such as disabling the auto preview feature in Microsoft Outlook, disabling windows scripting and other reported vulnerabilities.

Virus Removal/Notification Procedures:

If a virus-scanning program detects a virus and/or if users suspect infection by a computer virus, the user must immediately stop using the involved computer and notify their systems administration staff. Because viruses can be very complex, users shall not attempt to eradicate them from their systems unless they are authorized. The systems administration staff shall ensure that the anti-virus software on the computing device is brought up-to-date, a full scan performed, and necessary disinfection procedures are taken.

The systems administration staff will immediately disconnect the infected machine from all networks. The machine will not be reconnected to the network until systems administration staff can verify that the virus has been removed. If it cannot be removed, all software on the machine will be deleted including boot records if necessary. The software will then be reinstalled and re-scanned for viruses.

The systems administration staff must complete form [COT-F012](#), Security Incident Reporting form, which can be found at http://technology.ky.gov/support/cot_forms.htm. The systems administration staff must also report the virus activity to the Commonwealth Service Desk (502/564-7576) with the following information:

- Contact name and number;
- Type of system that's affected (desktop, workstation, server, etc.);
- Extent of infection;
- Anti-virus software and version installed on the infected system; and
- Any other pertinent information relating to the virus.

Resources:

- State's Anti-Virus Website:
<http://technology.ky.gov/security/default.htm>
- McAfee Anti-Virus Information:
http://technology.ky.gov/security/mcafee_info.htm
- COT's ftp Site:
<ftp://sunset.state.ky.us/pub/virus>
- COT-F012, Security Incident Reporting form:
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-1921/>
- COT Security Forms:
http://technology.ky.gov/support/cot_forms.htm