Education and Workforce Development Cabinet
POLICY/PROCEDURE

Policy Number: EDU-011

Effective Date: June 01, 2002
Revision Date: December 20, 2012

Subject: Anti-Virus Policy

Policy: This policy supports the Education and Workforce Development Cabinet's (EDU) standard 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

EDU is responsible for designating technical contacts for virus-related issues. These contacts have access to McAfee's technical support for problems that cannot be addressed by them and/or Commonwealth Office of Technology (COT).

The EDU desktop administration staff is responsible for ensuring that the virus protection software has been installed and is functioning properly (services running) on all computing equipment.

Office managers are responsible for their agencies' compliance to the Anti-Virus Policy, as well as all Cabinet's policies. Failure to police their staff could result in a loss of networking services for offending offices.

COT Responsibilities

COT administers the enterprise agreement for virus protection software that exists between the Commonwealth of Kentucky and McAfee of Network Associates, Inc. The site license for the Total and Active Defense Products entitles participants to also install these products on home computers.

While anti-virus software can be downloaded from licensed participants at Network Associates' website at www.nai.com, COT also maintains an anti-virus website at ftp://sunset.state.ky.us/pub/virus/, for such software and other pertinent anti-virus information. The McAfee Enterprise licensing participants are able to download anti-virus software from the website by first obtaining the password from a member of the COT Virus Defense Team, 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: The EDU Security Audit Group (SAG) is responsible for the maintenance of this policy. The Chief Information Officer (CIO) is responsible for the revision of the EDU Policy and Procedures Manual (PPM). The EDU CIO is responsible for authorizing all changes to the PPM.

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 these computers connecting to the state network meet the same standards as computers in the workplace. The site license for the Total and Active Defense Products entitles participants to also install these products on home computers. 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 floppy disks 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 NAI's McAfee 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.

Step 3. Routine full scans of all files on servers and workstations, as well as DAT (virus definition file) updates and engine/software upgrades, shall be scheduled regularly, at least weekly.

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 EDU-F01. The systems administration stall also must report the virus activity to the EDU's Help Desk (502/564-9216) 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.

Review Cycle:
Annually

Timeline:
Review Date: November 29, 2012
Reviewed By: EDU Agency Security Contacts

Enterprise Security and Policies
Cross Reference:
http://technology.ky.gov/governance/Pages/policies.aspx
CIO-073 -- Anti-Virus Policy

OTS Standards
Cross Reference:
EDU-F01 – Security Incident Report Form