

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

Policy Number: CIO-073

Effective Date: 06/01/2002

Revision Date: 03/23/2015

Reviewed Date: 03/23/2015

Subject: Anti-Virus Policy

Policy Statement: This policy supports the best practices, standards, and guidelines for security that must be followed to protect the Commonwealth. The purpose of this policy is to help protect computing devices (servers, desktops, laptops and tablets) from malware (viruses, trojans, worms, hoaxes, etc.).

Policy Maintenance: The Commonwealth Office of Technology (COT), Office of the Chief Information Security Officer, has the responsibility for the maintenance of this policy. Organizations may choose to add to this policy as appropriate, in order to enforce more restrictive standards. Therefore, staff members are to refer to their organization's internal policy, which may have additional information or clarification of this enterprise policy.

Authority: KRS 42.726 authorizes the Commonwealth Office of Technology to develop policies that support and promote the effective application of information technology within the Executive Branch of state government, as well as information technology directions, standards, and necessary management processes to assure full compliance with those policies.

Applicability

This policy is to be adhered to by all Executive Branch agencies and staff, including employees, contractors, consultants, temporaries, volunteers and other workers within state government.

Responsibility for Compliance: Each Agency is responsible for assuring that appropriate staff within their organizational authority have been made aware of the provisions of this policy, that compliance by the staff is expected, and that unauthorized and/or neglectful actions in regard to this policy may result in disciplinary action pursuant to KRS 18A up to and including dismissal. It is each Executive Cabinet's responsibility to enforce and manage the application of this policy.

Non-compliance to the policy may result in additional shared service charges to the Agency for COT's remediation efforts pertaining to this policy. Failure to comply may also result in termination of that Agency's access to the network infrastructure.

Review Cycle: This policy will be reviewed at least every two years.

Policy: Computing devices (servers, desktops, laptops and tablets) must be scanned for malware. See [enterprise architectural standard 5530](#) for approved products. For consolidated agencies, COT is responsible for supporting the agency and ensuring appropriate malware protection software has been installed and is functioning on devices. For non-consolidated agencies, the agency administrator is responsible.

If a home computer is used to access state resources, agencies and staff must ensure that computers connecting to the state network meet the same malware protection standards as computers in the workplace.

Only approved software is allowed to reside on Commonwealth of Kentucky owned computer resources. Authorized individuals should install such software. This practice will help minimize the risk of malware being introduced into the Commonwealth of Kentucky computing environment. For approved software, please see the 2000 Software Domain of [Enterprise Architecture and Standards](#).

If a virus-scanning program detects malware and/or if a user suspects infection, the user must immediately stop using the involved computer and notify the Commonwealth Service Desk by calling (502) 564-7576. The machine will not be reconnected to the network until necessary disinfection procedures are taken and/or the device is re-imaged. For security best practices, please view the Security Awareness Video located on the [Cyber Security Training and Awareness](#) web page.

References:

- Enterprise Architecture and Standards :
<http://technology.ky.gov/governance/Pages/OverviewofenterpriseITPolicyStandards.aspx>
- Cyber Security Training and Awareness -- Security Awareness Video:
<http://technology.ky.gov/ciso/Pages/CyberSecurity.aspx>

END