Policy Title and #	CIO-073: Anti-Virus Policy				
Effective Date:	06/01/2002	Revision Date:	03/08/2017	Review Date:	09/01/2021

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 Commonwealth owned devices from malware.

DEFINITIONS:
Malware: Any type of malicious software including but not limited to viruses, trojans, etc.

POLICY:
All Commonwealth owned computing devices (servers, desktops, laptops and tablets) must be scanned for malware. Only IT products listed within the Kentucky Information Technology Standards (KITS) are approved for installation and use. For consolidated agencies, authorized COT individuals are responsible for supporting the agency and ensuring appropriate malware protection software has been installed and is functioning on devices. For non-consolidated agencies, the authorized agency administrator is responsible for ensuring appropriate malware protection software has been installed and is functioning.

If a virus-scanning program detects malware and/or if a user suspects an 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.

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 internal policies as appropriate and necessary. 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.

REFERENCES:
Helpful references can be found on the Enterprise IT Policies webpage.