



OIT 62.405: Malicious Code Protection

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

The Malicious Code Protection policy defines the steps necessary to provide adequate and effective protection for University systems.

II. Purpose

The Malicious Code Protection policy identifies controls to protect IT systems from damage caused by malicious code.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

NSU shall, or shall require that its service provider:

1. Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spy-ware, keystroke loggers, phishing software, Trojan horses, etc.).
2. Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.
3. Provide malicious program detection, protection, eradication, logging, and reporting capabilities.
4. Provide malicious code protection mechanisms via multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.

Example: The University may elect to provide protection against malicious code transmitted via email on the email servers and on the desktop.

5. Provide protection against malicious programs through the use of mechanisms that:
 - a. Eliminates or quarantines malicious programs that it detects;
 - b. Provides an alert notification;
 - c. Automatically and periodically runs scans on memory and storage devices;
 - d. Automatically scans all files retrieved through a network connection, modem connection, or from an input storage device;
 - e. Allows only authorized personnel to modify program settings; and
 - f. Maintains a log of protection activities.
6. Provide the ability to eliminate or quarantine malicious programs in email messages and file attachments as they attempt to enter the University's email system.
7. Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available, and propagate the new files to all devices protected by the malicious code protection program.
8. Require all forms of malicious code protection to start automatically upon system boot.
9. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.
10. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shutdown, restoration, notification, and reporting requirements.
11. Require use of only new media (e.g., diskettes, CD-ROM) or sanitized media for making copies of software for distribution.
12. Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.
13. By written policy, prohibit the installation of software on University IT systems until the software is approved by the Information Security Officer (ISO) or designee and, where practicable, enforce this prohibition using automated software controls, such as Active Directory security policies.
14. Establish Operating System (OS) update schedules commensurate with sensitivity and risk.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.