Policy Title: Malicious Code Protection

Policy Type: Administrative


Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Malicious code protection addresses the intrinsic nature of information systems to be targeted with software or code with virulent intent and the necessary measures for mitigating these threats to the University’s information system and its components.

TABLE OF CONTENTS

| Contacts | 1 |
| Purpose | 2 |
| Requirements | 2 |
| Violations | 4 |
| Interpretation | 4 |
| Publication | 5 |
| Review Schedule | 5 |
| Related Documents | 5 |

CONTACT(S)

Office of Information Technology – (757)823-2869
STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology

PURPOSE

This policy is intended to establish the policy and procedures for the protection from malicious code on the University’s information system and its components.

REQUIREMENTS

NSU:

1. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
   a. Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
   b. Inserted through the exploitation of information system vulnerabilities;

2. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with University configuration management policy and procedures;

3. Configures malicious code protection mechanisms to:
   a. Perform periodic scans of the information system at least once a week and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with University security policy; and
   b. Quarantine malicious code; send alert to administrator; in response to malicious code detection; and

4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

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, spyware, 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 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.

4. Provide protection against malicious program 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.

5. 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.

6.Require all forms of malicious code protection to start automatically upon system boot.

7. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.

8. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shut-down, restoration, notification, and reporting requirements.

9. Require use of only new media (e.g. diskettes, CD-ROM) or sanitized media for making copies of software for distribution.

10. Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.

11. 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.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect University missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, the University must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.

Control Enhancements for Sensitive Systems:

1. The University centrally manages malicious code protection mechanisms.

2. The information system automatically updates malicious code protection mechanisms (including signature definitions).

The information system prevents non-privileged users from circumventing malicious code protection capabilities.

VIOLATIONS

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 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.

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.
PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;

2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;

3. Post the policy on the appropriate SharePoint Site and/or Website; and

4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:

- Supersedes (previous policy): OIT 62.8.1703 Malicious Code Protection

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard