
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *Malicious Code Protection*

In accordance with the [COV ITRM 501-01](#), malicious code protection is necessary to protect System Office and College IT systems from damage caused by malicious code. Malicious code refers to a broad category of software threats to your network and systems and may exploit vulnerabilities in System Office and College IT systems. Deliberate destruction, theft, or unauthorized access or modification exploits or damages IT systems

Requirement:

System Office and College must develop standards and procedures that inform employees of their responsibility concerning malicious programs and explicitly prohibit:

- Intentional development or experimentation with malicious programs.
- Intentional propagation of malicious programs.
- Instructions on how users should respond to malicious attacks including reporting requirements.

These issues are addressed in SVCC's Security Awareness Training program, and by the Employee Ethics Agreement, Student/Patron Acceptable Use Agreement, Personnel Security Standard and, Information Security Standard. (Section H 2 and Attachment H 2.1 respectively)

System Office and College standards and procedures must also address the following:

- Instructions on how IT personnel will respond to malicious attacks. This information is contained in the Threat Detection: *Incident Handling* standard. (Section I 2)
- Instructions on using sanitized or new media to make software copies for appropriate distribution. This issue is addressed in the It Systems Security: *Malicious Code Protection, Procedure for Creating Distribution Media* document. (Attachment D 3.1)
- Instructions on using common use workstations, desktop, classrooms, labs, etc. to create distribution media. This issue is addressed in the It Systems Security: *Malicious Code Protection, Procedure for Creating Distribution Media* document. (Attachment D 3.1)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *Malicious Code Protection*

SVCC includes information for students on proper media use and the dangers of malicious programs. SVCC also includes information for instructors, lab assistants, learning resource center personnel, and similar employees on creating a safe environment for students in open areas by providing malicious program information to students. This information is distributed via syllabus, signage, and the SVCC web site www.sv.vccs.edu. The SVCC Security Awareness Program, Employee Ethics and Student / Patron Agreements (Attachment H 2.1) address these issues as well.

- Instructions for employees when purchasing new software or installing existing software to include Information Security Officer (ISO) or designee approval and installation procedures. These procedures are outlined in the IT Asset Management: *Change Management and Configuration Control*, and *Software License Management* standards and associated forms. (Sections J 2 and J 3).

The SVCC Security Awareness and Training Program include malicious code best practices for users. Email notifications and web site information may also be used to inform users of new viruses, worms, spy ware, and similar malicious programs. (SVCC uses MOAT for its Security Awareness and Training program). Removed in the July 2007 revision of the COV ITRM 501-01

Requirement:

SVCC must take every precaution to provide protection against malicious programs by using detection, protection, elimination, logging, and reporting capabilities. The following best practices are provided to the System Office and Colleges: SVCC uses Norman and Symantec Anti-Virus, and Zone Alarm spyware/firewall protection applications to satisfy the above and below requirements.

- Configure malicious code protection to activate upon system boot.
- Configure networks so that malicious codes are detected and removed or quarantined before it can impede a production device.
- Configure e-mail systems to eliminate or quarantine malicious programs in e-mail messages and file attachments as they enter the system.
- Have messages scanned by multi-vendor anti-virus programs (i.e., a firewall that uses multiple virus scanning engines).
- Configure systems for automatic updates of malicious code definition files or provide a process to manually retrieve those updates as they become available.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *Malicious Code Protection*

- Propagate malicious code definition file updates to all devices appropriately.

SVCC Malicious Code Protection using the applications mentioned above encompasses the technologies and processes available to:

- Eradicate or quarantine malicious programs detected.
- Send alert notifications.
- Run scans on memory and storage devices.
- Scan files received via a network or other connection or from an input storage device.
- Allow only authorized employees to modify program settings. This is addressed in the Personnel Security: *Access Determination and Control* standard. (Section H 1)
- Maintain a log of malicious program protection activities. SVCC IT Staff will document and maintain all log files.