In accordance with the VCCS Security Standard 10.4, 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: Controls Against Malicious Code §10.4.1**

VCCS and Colleges will protect information by implementing detection, prevention, and recovery controls against malicious code. VCCS and Colleges will implement appropriate user awareness procedures and programs to educate users on the risks and responses to malicious code.

In addition, VCCS and Colleges may consider the use of two or more software products protecting against malicious code across the information processing environment from different vendors can improve the effectiveness of malicious code protection. Care will also be taken to protect against the introduction of malicious code during maintenance and emergency procedures, which may bypass normal malicious code protection controls.

In meeting this requirement, SVCC has adopted the following controls:

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 anti-virus and spyware detection software along with 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.
IT Systems Security – *Malicious Code Protection*

- 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.
- 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.
- Maintain a log of malicious program protection activities. SVCC IT Staff will document and maintain all log files.

SVCC 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 Acceptable Use Agreement](#), [Student/Patron Acceptable Use Agreement](#), [Personnel Security Standard](#), and [Information Security Standard](#).

- See [SVCC Security Policies](#), Policy 10.1.1, *Virus Protection*
- See [SVCC Security Policies](#), Policy 4.1.4, *Malicious Code Protection*
- Also see SVCC *Malicious Code Protection* document, Section J 3, SVCC Security Plan. Location: Security\SVCC ISO 27002 2011\Phase III documentation\SVCC Phase III\10 Communications and Operations Management\J Asset Management
- See [SVCC Security Policies](#), Policy 8.1.1, *Security Awareness and Training*
IT Systems Security – *Malicious Code Protection*

**Requirement: Controls Against Mobile Code §10.4.2**

VCCS and Colleges will protect information by ensuring that where the use of mobile code is authorized, the configuration operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.

Security awareness programs will describe mobile code as software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction and is associated with a number of middleware services.

In addition to ensuring that mobile code does not contain malicious code, control of mobile code is essential to avoid unauthorized use or disruption of system, network, or application resources and other breaches of information security.

In meeting this requirement, SVCC has adopted the following controls:

- See requirement 10.4.1 above
- Executing mobile code in a logically isolated environment
- Control the resources available to mobile code access (i.e. email, web traffic only)

  - See [SVCC Security Policies](#), Policy 10.1.1, *Virus Protection*
  - See [SVCC Security Policies](#), Policy 4.1.4, *Malicious Code Protection*
  - Also see [SVCC Malicious Code Protection](#) document, Section J 3, SVCC Security Plan. Location: Security\SVCC ISO 27002 2011\Phase III documentation\SVCC Phase III\10 Communications and Operations Management\J Asset Management
  - See [SVCC Security Policies](#), Policy 8.1.1, *Security Awareness and Training*