

Virginia Commonwealth University Technology Services

Public Computer Facility Security Standard

Definition:	<i>This standard applies to computers that are in a facility that is used by the public (i.e., non-VCU users).</i>
Designation:	Technology Services Standard
Effective Date:	February 15, 2006
Review Frequency:	Annually or as needed
Authority:	VCU Chief Information Officer VCU Security Officer
In Compliance with:	VCU Academic Policy: Security of Electronic Sensitive Information VCU Academic Policy: Information Security Policy UITAC Goals: <i>Infrastructure Goal 3.</i> COV ITRM Information Technology Security Management Standard SEC501-01 VCU Computer and Network Resources Use Policy

Scope:

This standard applies to all University public personal computer facilities that are not restricted to VCU users only. These facilities are accessible by anyone associated with VCU and by the greater community (i.e., non-VCU users).

Computer labs that are restricted to use by VCU personnel and are not used for classroom activities must follow the [Computer Lab Security Standard](#).

Computer labs that are used for classroom activities must follow the [Computer Classroom Security Standard](#).

Applied Industry Best Practices of:

- National Institute of Standards Technology (NIST)

Requirements of the Standard.

1. Prevention of the Installation of Malware

Each facility must implement steps to prevent malicious code from being installed and executed on the lab computers. Centralized desktop management software must be used to automatically distribute security updates, monitor for security threats, and remediate problems that occur on the lab computers.

2. Restriction of Privilege

The principal of least privilege must be followed on public computers, and the local logon account should not have administrator privilege.

3. Current Security Software

The latest desktop security software available (e.g., anti-virus software) from Technology Services must be installed and kept up-to-date on all computers.

4. Physical Security

All computer facilities should be physically checked for unauthorized hardware devices (such as hardware key loggers) on a periodic basis. The frequency and completeness of these checks should be more for facilities that do not have physical controlled access or monitoring.

5. Signage

There should be a standard system banner (see #5 under Implementation Guidelines). In addition, there should be visible signage warning the users that the computers will be reset and that they should practice safe computer and not enter their personal information on public computers.

Implementation Guidelines

1. Prevention of the Installation of Malicious Code:

A) Centralized desktop management software must be used in the facility. The following are some suggested products:

- a) LANDesk
- b) Microsoft Imaging
- c) ZENWorks for Desktops

B) Disallowing the installation of software by policy restrictions can be used to prevent malware from being installed. Public PCs can be members of an Active Directory OU(s) to limit activity via Active Directory group policy (GPO).

C) Resetting software such as Deep Freeze by Faronics can be used to control and limit the exposure to malware, and whitelist technology such as Anti-Executable by Faronics can be used to prevent the installation of unauthorized software. Deep Freeze returns the computer to its original state, and Anti-Executable prevents the execution of unauthorized programs.

D) Microsoft Shared Access is another alternative. Available as a free add-in from Microsoft, this utility allows an administrator to control the PC's valid image by defining a restore point in the local group policy.

E) CheckSeelfRunning.exe, A VB Script developed by Technology Services, can be installed and modified to include the filename extension of any software that is considered malware by lab managers. The script resides on the PC and loads into RAM while the PC is operational. If unauthorized software is detected by this script, the PC automatically reboots.

F) Thin clients can be installed in these facilities.

G) Other technologies that become available such as Microsoft's Shared Computer Toolkit and desktop virtualization security solutions (e.g., the use of VMWare) as long as the technology achieves the stated goal of preventing malicious code from being installed and executed on the lab computers.

2. Restriction of Privilege

The local logon account for the computer should not have excessive privilege since that puts the machine and user of the machine at risk for infection. If certain software is being used in this facility that requires administrative privilege, [DropMyRights](#) should be used on all Internet accessing software (e.g., browsers) to restrict the exposure to malware that is possible when visiting malicious websites.

3. Current Security Software

Check the VCU security website for information on the latest available software: <http://www.ts.vcu.edu/security/>

Security software such as the latest version of the anti-virus software provided by VCU must be installed on each computer and the definitions files must be up-to-date.

Other security software such as anti-spyware software should also be installed.

4. Physical Security

All computers should be secured through cabling, locks, etc. to enhance physical security. If possible, access to the public facility should be monitored either through electronic means (card swipe, security camera, web cam, etc.) or by a designated lab monitor technician.

The computer chassis should be arranged so that there is not easy access to the rear where hardware devices could be installed and not obviously visible.

In addition, physical checks of the computers for unauthorized attached devices should be conducted frequently. The suggested schedule is at least weekly for public facilities; however in situations where there are large number of computers and it is not feasible to perform weekly physical checks, checks should be done as frequently as possible.

5. Signage

The following is a standard system banner to be used on public computer facility workstations:

Use of this computer constitutes consent to the appropriate use standards set forth in the VCU Computer and Network Resources Use Policy (<http://www.ts.vcu.edu/policies/computeruse.html>). All other use is prohibited. All information on this computer system may be monitored by authorized University personnel for official purposes as permitted by state and federal law.

Signs should also be posted on the desktop or near each computer advising users that the machines will be reset periodically and that they should follow safe computer practices and not enter personal information on public computers.

Enforcement

Public PC facilities at the University will be periodically checked to ensure that they are abiding by the requirements set forth in this standard. In cases where the computers are not being properly secured and end users and University network resources are threatened, Technology Services may act on behalf of the University to eliminate the threat by working with the relevant computer facility owner or overseer to quickly close security holes. In circumstances where these collaborative efforts fail or there is an urgent situation requiring immediate action and leaving no time for collaboration, the public computer facility may be closed and the computers may be disconnected from the network by VCUNet.

Exceptions

Requests for exceptions to the requirements of this standard should be made in writing (by hard copy or email) to the VCU VP/CIO.

Revision History:

September 17, 2006: Edits

November 18, 2006: Edits