

Virginia Commonwealth University Technology Services

Computer Lab Security Standard

Definition:	<i>This standard applies to general personal computer labs that are restricted to VCU use only and that not used for classroom activities.</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 general personal computer labs that are restricted to VCU users and are not used for classroom activities.

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

Computer facilities that are open to the public (i.e., non-VCU users) must follow the [Public Computer Facility Security Standard](#).

Applied Industry Best Practices of:

- National Institute of Standards Technology (NIST)

Requirements of the Standard

1. Authentication and Tracking

Lab computers connected to the VCU Network must have an authentication mechanism that uniquely identifies the user of the computer for each session. Before using the lab computer, each user will be required to authenticate with their unique user ID and password credentials. Some method of session time out must be enabled for the user accounts, and a method of logging who is using the computer at any given time must be enabled.

2. Prevention of the Installation of Malware

Each PC Lab 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.

3. Restriction of Privilege

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

4. Current Security Software

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

5. Physical Security

All PC Labs 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 labs that do not have physical controlled access or monitoring.

6. Signage

There should be a standard system banner (see #6 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 semi-public or public computers.

Implementation Guidelines

These guidelines are options or suggestions for implementing the requirements of the Computer Lab Security Standard. While lab managers have flexibility in how the standards are implemented, deviations from recommended guidelines should be reasonable, supported and not expose users to unnecessary risk.

The VCU Technology Services Information Security Officer (ISO) will review the implementation of the standards in all labs and assess the effectiveness of locally-developed solutions. If local measures are deemed to not provide sufficient user security, lab managers will be required to implement more secure measures under the guidance of the ISO.

1. Authentication and Tracking:

A) The first guideline option is to implement a utility called The Authenticator. This utility was developed by Technology Services to force a login and password entry on a PC. An end-user must use his or her eID/password combination to authenticate to the network for successful login. When the user logs out of the PC, a system reboot is automatically initiated.

The eID/password combination is date stamped and kept for audit purposes in case of compromise. The logs can be monitored by authorized staff and are useful for investigative purposes if there are any security problems with lab computers.

B) The second option is to use the authentication tools provided for the PCs native operating system (OS). Windows, Mac OS, UNIX, and Linux offer add-ins that permits the end-user to authenticate to LDAP (eDirectory).

C) A card-swipe using the VCUCARD solution can be implemented at each lab workstation as a third option.

- D) If the computer lab machines are logging into into eDirectory (VCU tree) or Active Directory, that log in should be unique to the individual using the computer and not a universal login. If a universal login is used, it should be used **in addition** to the Authenticator program described in A) above so that the individual using the computer can be identified.

Whatever authentication method is used, there should be a session timeout function which logs off the workstation if there is a period of inactivity.

2. Prevention of the Installation of Malicious Code:

A) Centralized desktop management software must be used in the labs. 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 lab 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) CheckSelfRunning.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 open labs.

- 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.

3. Restriction of Privilege

The local logon account for the lab computers 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 the lab 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.

4. 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 lab computer and the definitions files must be up-to-date.
Other security software such as anti-spyware software should also be installed.

5. Physical Security

All open lab PCs should be secured through cabling, locks, etc., to enhance physical security. Access to the lab 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 lab workstations for unauthorized attached devices should be conducted frequently. The suggested schedule is a daily check for general open access labs.

6. Signage

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

This computer and all University systems accessed from it are for official University use as authorized by 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 personnel for official purposes. Access or use of this computer system by any person constitutes consent to this policy.

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 semi-public or public computers

Enforcement

University computer labs will be periodically checked to ensure that they are abiding by the requirements set forth in this standard. In cases where labs 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 lab 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 lab 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 (hard copy or email) to the VP/CIO.

Revision History:

August 11, 2006: Clarification of guidelines

September 17, 2006: Additional requirement

November 16, 2006: Edits