

Enhanced Security Management for Desktop/Notebook Computers

Version: 1.1

Status: *Approved*

Effective Date: 07/01/08

Contact: [Director, Technology Administration Services](#)

PURPOSE

The VCCS provides shared information technology resources and services to faculty, students, staff, and college patrons for activities supporting the VCCS mission. The purpose of this standard is to ensure the IT resources used specifically in support of academic instruction and research systems follow the educational industry best practices for protecting endpoints.

SCOPE

The following standard describes some specific risks associated with the granting of administrative rights to a notebook or desktop computer. It further outlines the associated controls that must be in place no later than July 1, 2009 before granting administrative rights on an individual notebook or desktop computer. Computers used in the classrooms and student labs are exempted from this standard.

APPLICABILITY

This standard is applicable to the System Office and all colleges.

DEFINITION

Academic instruction and research systems, as noted in the SEC501-01 Security Standard, are defined as those systems used by institutions of higher education for the purpose of providing instruction to students and/or faculty for the purpose of conducting research. As such, these systems are exempt from the requirements of the Standard. For VCCS purposes, academic instruction and research systems include the desktop computers, notebook computers, computer labs, classrooms, and related infrastructure used by the college teaching faculty, teaching assistants, and instructional technologist providing direct instructional support to the students and faculty.

STANDARD

In accordance with the VCCS Information Security Standard, notebook and desktop computers used in support of academic instruction and research systems can be granted administrative rights, and support the use of non COV owned mobile devices. All authorized individuals granted administrative rights under this standard will be required to follow and adhere to all local college

policies and procedures that maybe derived from this guidance. However, the following also applies:

Major Risks & Controls

Risks are associated with using computers to conduct the business activities; as such they can have intentional and unintentional consequences. If they are intentional then it is quite possible that the best controls may be defeated. However, risk assessment remains a critical activity in protecting Information Technology resources. Therefore the following are list of the risks normally associated with the use of desktop and notebook computers and the controls that are required by this standard:

1. Administrative Rights Activation
 - a. Administrative rights are considered as “privileged accounts” therefore the college must include the formal activation process within their current procedures for requesting and granting access to IT services. As a minimum, there should be a formal review of each request and appropriate signoffs.
2. Installation of malicious code software (viruses, root kits, Trojans, keyloggers, etc)
 - a. Install the approved anti-virus software
 - b. Automate the maintenance of the supporting antivirus definitions
 - c. Maintain current operating system fixes and updates
 - d. Develop and enforce standards for protecting from malicious code through manual process or through automated means such as implementing Network Access Control (NAC) to validate certain controls (i.e. AV) are implemented before or while the device is connected to the network
3. Changes to the security configuration of the system making the system more vulnerable to attack.
 - a. Implement configuration monitoring through manual process such as file verification or through an automated solution such as desktop reimaging or Tripwire
4. Installation of unapproved patches that could compromise the stability of the system
 - a. Control by policy, enforce through audit logging and review
5. Installation of unlicensed software
 - a. Control by policy, enforce through audit logging and review or through a software inventory solution such as Altiris
6. Installation of security tools such as vulnerability scanners or penetration tools that can cause network congestion or crash systems.
 - a. Control by policy, enforce through audit logging and review
7. Minimize access to the computer
 - a. Use password protected screensavers set for a maximum of 15 minutes
 - b. Physically secure the computer where possible
8. Storage of confidential and/or sensitive information
 - a. Information must be encrypted using an approved endpoint security solution
 - b. There must be documentation supporting the need
 - c. Must have agency head approval
9. User Security Awareness and Training
 - a. Those assigned this privilege must complete training that is commensurate with the level of access granted

Controlling access to local administrative rights is a portion of a layered security model or defense-in-depth strategy. Colleges and System Office should conduct an assessment for each application of this standard.

RELATED LINKS: [Information Security Standard](#)