
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security - *IT System Hardening*

In accordance with the [COV ITRM 501-01](#), IT system hardening is necessary to protect System Office and College IT systems against vulnerabilities.

IT system hardening focuses on the technical security controls of IT systems. It does not apply to sensitive or high risk systems only but to **all** IT systems.

Requirement:

The System Office and Colleges should apply appropriate baseline security configurations to all IT systems. These configurations are to include malicious code protection, operating system and application software patches and / or upgrades. For IT systems that have been identified as high risk or that contain sensitive and confidential data, security configurations should be more restrictive. SVCC is using the template (where applicable) as suggested per the VCCS Technology Guidelines: *Security Guidelines for LAN's* http://system.vccs.edu/its/security/Security_Guideline_for_LAN.htm and the Technology Guidelines: *Security Guidelines for Windows 2000* http://system.vccs.edu/its/security/Security_Guideline_for_Windows_2000.htm standards (Attachment D 1.1) to develop appropriate security configurations.

In addition, users will have their accounts based on the premise of “least privilege”, screensavers will be password protected, and the Remote Desktop Connection feature will be disabled on all Windows XP and Vista operating systems. All security configurations must be documented and maintained on file. The IT Staff at SVCC will document and maintain all security configurations, operating system and application software patches and / or upgrades. The following websites may be used for additional information regarding security configurations:

The VCCS Security Website

<http://www.vccs.edu/its/security/index.htm>

The Center for Internet Security

<http://www.cisecurity.org/sitemap.html>

NIST Security Configuration Checklists Repository

<http://checklists.nist.gov/repository/category.html>

Requirement:

Once security configurations, operating system and application software patches and / or upgrades have been applied and documented, they should be reviewed annually or more

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security - *IT System Hardening*

frequently as applicable. The SVCC IT Network Administrator must monitor systems for security baselines and policy compliance. (Jan 2010 Revision) Security configurations should be re-applied when a system is changed (a system upgrade for example). The IT staff will do preliminary review. The final, formal review will be conducted annually before June 15 by the SVCC IT Security Committee using the IT Systems Security: *IT Systems Hardening*, Security Configurations Review form. (Attachment D 1.1) The college ISO will maintain the completed forms for audit purposes.

Requirement:

The SVCC IT Staff will do Vulnerability scanning of IT systems a minimum of once annually before June 15, and more often as is deemed necessary. The VCCS also does Vulnerability scanning of college IT systems periodically to ensure security configurations remain in place and are adequate for the sensitivity and risk associated with the IT system.

Modifications will be made if security configuration effectiveness is insufficient based on the vulnerability scanning. The updated configurations will be documented and maintained on file by the VCCS IT Staff, as a part of the annual review process. Additionally, any exploits will be reported to the ISO as per the Threat Management: *Incident Handling* standard.