
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Remote Access*

In accordance with the [COV ITRM 501-01](#), Remote Access standards and procedures must be implemented to ensure the steps necessary for providing for the secure use of remote access to Systems Office and College IT systems and data.

Simply stated, remote access is the ability to get access to a computer or a network from a remote distance. Security measures for remote access should be implemented based on sensitivity and risk to System Office or College IT systems and data. The SVCC IT Network Administrator is responsible for compliance with and documentation of all requirements as given in this standard.

Requirement:

The System Office and SVCC procedures document user requirements for use of remote access and the need for remote access to sensitive data. This includes:

- Employee procedures for requesting remote capabilities including supervisor or administrative approvals if required. This is addressed in the Logical Access: *Account Management*, and Personnel Security: *Access Determination and Control* standards, using the SVCC Account Applications Request form. (Sections E1 and H1 respectively)
- User ID assignments (a unique user ID assigned or use of current user ID) depending on the type of remote access used and additional security measures already in place. This is addressed in the Logical Access: *Account Management*, and Personnel Security: *Access Determination and Control* standards. (Sections E1 and H1 respectively)
- Provide security awareness and training and instruction on remote access prior to a user receiving such access. SVCC uses the M.O.A.T. Security Awareness and Training program.

Requirement:

An important consideration when establishing remote access connections is encryption. The security of remote access to the System Office or College IT systems and data must be in compliance with the [Data Protection, Encryption Standard](#). (Attachment E 3.1) This includes the remote file transfer of sensitive data to and from VCCS systems.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Remote Access*

Requirement:

The System Office and Colleges must document the requirements for physical and logical hardening of remote access devices. This requirement is met in the Systems Security: *Systems Hardening* standard, Section D 1 SVCC Security Plan.

Requirement:

Remote access records must be maintained for audit purposes in accordance with current System Office and College records retention policies. This is addressed in the Logical Access: *Account Management*, and Personnel Security: *Access Determination and Control* standards. (Sections E1 and H1 respectively) Also in Section D2, IT System Security: *IT Systems Interoperability* standard.

Requirement:

Where supported by features of the system, session time outs shall be implemented after a period of not longer than 30 minutes of inactivity and less commensurate with sensitivity and risk. (Jan 2010 Revision)