
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Account Management*

In accordance with the [COV ITRM 501-01](#), Account Management standards and procedures must be implemented to ensure the steps necessary for requesting, granting, administering, and terminating accounts at the Systems Office and colleges are formalized.

An account generally consists of a user ID and a password and supplying this account information will grant the user access to a set of resources and services based on the request and proper approvals. The requirements and recommendations below establish best practices for administration of accounts that provide access to System Office and College IT systems. [This standard establishes access requirements for internal and customer-facing IT Systems. Internal IT systems are designed and intended for use by VCCS employees, contractors, vendors, and third parties. Customer-facing IT systems are designed and intended for use by VCCS customers and by members of the public. VCCS employees, contractors, vendors, and third parties may also use customer-facing IT systems. \(Jan 2009 Revision\)](#)

Requirement:

SVCC grants user access [for internal and customer-facing IT systems \(Jan 2009 Revision\)](#) to IT systems and data based on the principle of least privilege. The principle of least privilege requires that a user be given no more privilege than necessary to perform a job. This requirement is addressed in the Logical Access Control: *Account Management*, Procedure for Granting Access document and associated forms. (Attachment E 1.1) LAN and local machine access is determined and documented by SVCC IT Staff.

The employee's supervisor and the Data Owner must authorize and approve access to the IT system. This process is outlined in the Logical Access Control: *Account Management*, Procedure for Granting Access document. (Attachment E 1.1)

Criminal background checks, if required, should be completed before, establishing an account. SVCC specifies that all positions shall require a criminal background check. This requirement is addressed during the hiring process and is documented by the Human Resources department as a part of said process.

SVCC will perform an annual review of all user accounts for sensitive IT systems to ensure the access remains accurate and proper. This review will be conducted annually by

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Account Management*

the appropriate supervisors and recorded on the employees EWP as per the Logical Access Control: *Account Management*, Procedure for Granting Access document and associated forms. (Attachment E 1.1)

SVCC has procedures in place that outline the steps personnel must take to notify the proper individuals (to include HR and the ISO) when user accounts are no longer required or when a user account should be updated based on a change in an employee's EWP core duties. Situations requiring a change may include termination, transfer, or changes in duties and each should be addressed in the procedures, as well as, who is responsible for each step of the process. The process is outlined in the Logical Access Control: *Account Management*, Procedure for Granting Access document and associated forms. (Attachment E 1.1)

- Access should be removed immediately for an employee involuntary termination, for individuals with permissions for systems with sensitive and/or confidential information, or individuals that serve in positions that provide “super” access (such as security administrators). All other departures should be removed within 5 business days. The entire process is measured from the initial date of the employee notification or termination.
- At the beginning of the Spring, Summer and Fall semesters, a review of all active adjunct faculty accounts will be completed by the college, with each adjunct identified as follows:
 - Active – No changes made.
 - Not Teaching – Access continues, advising role (SIS) should be removed within 5 days.
 - Inactive (not taught for 3 semesters) – Account will be disabled within 5 days.
 - Will Never Return – Account should be deleted within 5 days.
 - Adjunct faculty whose accounts have been disabled, may request account reactivation for one semester.
 - Reactivation after account deletion will require the same procedure as new account creation.

The college ISO will review adjunct faculty accounts on an annual basis to ensure compliance with these procedures. The college ISO (with the help of the SVCC Security Administrator for PeopleSoft and Human Resources department), should also make sure that the System Office ISO is notified about all account changes so that enterprise accounts can be terminated. (Jan 2010 revision)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Account Management*

Requirement:

Unusual IT system activities will be investigated by the System Owner and System Administrator as per the Threat Management: *Security Monitoring and Logging* standard. (Section I 3) Changes to IT system access level authorizations will be approved by the System Owner, System Administrator, and all appropriate access granting personnel. All records must be updated to reflect any changes in IT system access levels. [Any access needed for emergency or temporary use must be requested and documented according to standard practice. The request shall be maintained on file, and expire after a predetermined period based on sensitivity and risk. Approval must be granted by the System Owner and communicated to the ISO. \(Jan 2009 Revision\)](#) The process is outlined in the Logical Access Control: *Account Management*, Procedure for Granting Access document and associated forms. (Attachment E 1.1) LAN and local machine access is determined and documented by SVCC IT Staff.

Requirement:

Authentication and authorization requirements must be defined based on sensitivity and risk of the IT system and data. The process is outlined in the Logical Access Control: *Account Management*, Procedure for Granting Access document and associated forms. (Attachment E 1.1) LAN and local machine access is determined and documented by SVCC IT Staff. A username and complex password (as defined in the VCCS Logical Access Control – Password Management Standard) has been deemed the appropriate authentication mechanism based on the sensitivity and risk of VCCS systems.

SVCC requires local accounts to have username and password authentication, remote access (VCCS) account parameters are determined by the VCCS as per the IT Systems Security: *Systems Interoperability* standard. (Section D 2)

The System Office or College may consider additional authentication methods (examples include cryptographic, biometric authentication, tokens, etc.) based on sensitivity and risk.

VCCS internal and customer-facing system usage must require the following additional controls to ensure accounts are proper and remain current. These controls are addressed in the SVCC security plan, Section E, *Account Management*. Controls are as follows:

- Prohibiting the use of shared accounts. [Those systems residing on a guest network are exempt from this requirement. \(Jan 2010 Revision\)](#)
- [If the IT system is classified as sensitive](#), prohibit the use of guest accounts. [\(Jan 2010 Revision\)](#)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Account Management*

- Locking an account automatically if not used for a predefined period.
 - Disabling or deleting unneeded accounts, promptly. (Jan 2010 Revision)
 - Disabling or deleting inactive accounts after 90 days.
 - Configure applications to clear cached data and temporary files upon exit of the application or logoff of the system. (Jan 2009 Revision)
 - Prohibit the display of the last logon user ID on multi-user systems. Desktop and laptop systems assigned to a specific user are exempt from this requirement. (Jan 2010 Revision)
 - Prohibit the granting of local administrator rights to users. An Agency Head may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the Agency Head's explicit acceptance of defined unmitigated risks. (Jan 2010 Revision)
1. Employees who feel they cannot perform their job without administrative rights must document their reasons for needing these rights.
 2. All requests will be reviewed on a case-by-case basis using the current college procedures for requesting access, and may be appealed to a college review panel.
 3. If the request is denied the Systems Office or Colleges should have an appeal process. This governance model may include an appeal review process by the Information Security Plan Committee, an administrative committee, a committee made up of peers and other knowledgeable employees, or the President/Chancellor if the ISO originally denied the request. All appeals must be auditable and allow for a thorough and appropriate review of the user request.
 4. When administrative rights are given to an employee, a special administrative account must be setup for this person. This person would normally use their account without administrative rights, but when needed, would use their special account with administrative rights to perform tasks where administrative rights are required.
 5. The ISO and/or review panel must assess employees with administrative rights on an annual basis to determine if these personnel still require administrative rights, to determine how those administrative rights have been used, and to determine if administrative rights have been abused. (Jan 2010 VCCS revision)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Account Management*

Recommendations:

- Create a guest network that would not have access to sensitive information (classrooms, labs, etc, would be considered a guest network).
- Move employee computers to this network for personnel with administrative rights.
- Personnel could be given administrative rights for use only on the segmented network.
- Create a lab where faculty and staff could experiment with technology.

Requirement

Unneeded accounts should be retained in a disabled state in accordance with the System Office or College records retention policy. All IT accounts for persons no longer employed by SVCC will be deleted and all IT access will be terminated. These issues are addressed in the Personnel Security: *Access Determination and Control* standard, (SVCC security plan Section H 1) and by the Logical Access Control: *Account Management*, Procedure for Granting Access document. (Attachment E 1.1)

Requirement

Access levels should be associated with group membership when possible and require that all IT system users be a member of at least one user group. This requirement is addressed in the IT Systems Security: *Systems Hardening* standard. (Section D 1)

Requirement: (Jan 2009 Revisions)

VCCS Internal System usage must require the following:

- A documented request from the user to establish an account.
- Complete required background check before establishing account, or as soon as practical.
- Require job descriptions that accurately reflect job duties to define the system IT access required.
- Require confirmation of the account request and approval by the IT system user's supervisor and approval by the System Owner to establish accounts for sensitive IT systems.
- Require delivery of access credentials to the user based on information already on file.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Account Management*

- Promptly remove access when no longer required.

SVCC Logical Access Control: *Account Management*, Procedure for Granting Access document. (Attachment E 1.1)

Requirement: (Jan 2009 Revisions)

VCCS customer-facing IT (External) systems must require the following:

- Secure delivery of access credentials to users of all customer-facing IT systems.
- Confirmation of the user's request for access credentials based on information already on file prior to delivery of the access credentials to users of sensitive, customer-facing IT systems.
- Delivery of access credentials to users of sensitive, customer facing sensitive IT systems by means of an alternate channel, such as U.S. Mail.

For all service and hardware accounts:

- Document account management practices for all custom service accounts, including, but not limited to granting, administering and terminating accounts. (Jan 2010 Revision)

SVCC Logical Access Control: *Account Management*, Procedure for Granting Access document. (Attachment E 1.1)