
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Password Management*

In accordance with the [COV ITRM 501-01](#), Password Management standards and procedures must be implemented to specify the means for password use to protect System Office and College IT systems and data.

SVCC must document password management practices to ensure adequate password procedures are implemented to protect against IT system and account intrusions. The SVCC IT Staff will maintain all documentation of password management configurations. SVCC will follow password management best practices as provided below.

Requirement:

Ensure that account access to sensitive IT systems require a password. This includes local, remote access, and temporary accounts.

Requirement:

Utilize the password features of an IT system to:

- Force a user to choose a secure password initially and each time the password expires.
- [Require users of all sensitive IT systems, to include network systems, to change their passwords after a period of 90 days. \(Jan 2010 revision\)](#)
- [Users of MyVCCS and any related system are required to change their passwords after a period of 180 days. \(Jan 2010 VCCS revision\)](#)
- [Prevent the reuse of the same or similar passwords by maintaining the last 12 passwords used in the password history files. \(except My VCCS\) \(Jan 2010 VCCS revision\)](#)
- Suppress the display of passwords as they are entered.
- Implement a system so that passwords are not sent over the network in clear-text, where technically possible.
- [Require password complexity based on sensitivity and risk utilizing the following format:](#)

[Passwords should be at least three of the following four:](#)

- Alphabetic characters

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Password Management*

- Numeric characters
- Symbols
- Combination of upper case and lower case letters

Passwords must be at least eight characters in length

- Prohibit use of passwords that can be found in a dictionary. This includes hardware passwords. (Jan 2010 revision)
- Configure all sensitive IT systems to allow users to change their password at most, once per 2 hour period. (Jan 2010 revision)
- Prohibit the transmission of passwords without the use of encryption methods. Reference the VCCS Data Protection, Encryption Standard.
- Prohibit the inclusion of passwords as plain text in scripts.
- Prohibit the use of “Guest” or Shared accounts. Shared passwords shall not be used on any IT systems. (Jan 2010 Revision)
- Require passwords on mobile devices such as PDAs and smart phones. For mobile phones, use a 4 to 5 digit pin number.

Requirement:

SVCC will provide training to staff on password security awareness via M.O.A.T. to:

- Inform users to notify the ISO if they suspect passwords have been compromised.
- Require users to maintain exclusive control and use of their passwords.
- Inform users to not allow web browsers and other applications to "remember" user passwords.

Requirement:

SVCC IT System Administration Management will:

- Provide a unique initial password for each new user and deliver the password in a secure and confidential manner.
- Provide requirements, and instructions if necessary, for the user to immediately change the initial or any other default password.
- Replace forgotten initial passwords rather than re-issue.
- Prohibit group accounts and passwords on sensitive IT systems.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Logical Access Control – *Password Management*

- Allow only the IT system and its authorized administrator access to files containing passwords.
- Document and store hardware passwords securely.
- Incident handling procedures should include lost or compromised passwords and/or tokens.
- Continuity of operations dictates that at least two employees have administrative account access to each IT system.
- System Administrator's should have both an administrative account and at least one user account. System Administrator's should use the administrative account only when performing tasks that require those privileges.
- [Require passwords be set on device management user interfaces for all network connected devices. \(Jan 2010 Revision\)](#)
- Implement a screen saver lockout period after a minimum of 30 minutes of inactivity. [COV devices located in classrooms or public use areas would be exempt from the screen saver lockout. \(Jan 2010 VCCS revision\)](#)
- [Set an account lockout threshold for not greater than five invalid attempts with lockout duration of at least 15 minutes for COV devices. \(Jan 2010 Revision\)](#)