Logical Access Control – *Password Management*


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: (User password Management - §11.2.3)**

- Users are required to sign a statement to keep personal passwords confidential and, if applicable, to keep group passwords solely within the members of the group; this signed statement will be included in the terms and conditions of employment; [*VCCS Acceptable Use Agreement*](#)
- When users are required to maintain their own passwords they will be provided initially with a secure temporary password, which they are forced to change immediately at first logon;
- Establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;
- Temporary passwords will be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages is not allowed;
- Temporary passwords are unique to an individual and should not be guessable;
- Users must acknowledge receipt of passwords;

In meeting this requirement, SVCC has adopted the following controls:

SVCC IT System Administration Management will:
Logical Access Control – *Password Management*

- 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.
- Allow only the IT system and its authorized administrator access to files containing passwords.
- Document and store hardware passwords securely.

  - **VCCS Acceptable Use Agreement**
  - See [SVCC IT Security policies](#), policy 5.1.3, *Password Policy*

**Requirement: (Password use - §11.3.1)**

Users are required to follow good security practices in the selection and use of passwords, including the following:

- Keep passwords confidential;
- Avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;
- Change passwords whenever there is any indication of possible system or password compromise;
- Select quality passwords with a minimum length of 8 characters which are:
  - Easy to remember;
  - Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
  - Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
  - Free of consecutive identical, all-numeric or all-alphabetic characters;
Logical Access Control – *Password Management*

Require password complexity based on sensitivity and risk utilizing the following format:

Passwords should be at least three of the following four:

1. Alphabetic characters
2. Numeric characters
3. Symbols
4. Combination of upper case and lower case letters

- Change passwords every 90 days, (passwords for privileged accounts should be changed every 30 days), and prevent the reuse by maintaining the last 12 passwords used in the system’s password history file (except for MyVCCS);
- Passwords cannot be changed more frequently than once every two hours;
- MyVCCS passwords are required to be changed on a 180 day cycle;
- Change temporary passwords at the first log-on;
- Not include passwords in any automated log-on process, e.g. stored in a macro or function key, or displayed as they are being entered;
- Not share individual user passwords;
- Not use the same password for business and non-business purposes;
- If users need to access multiple services, systems or platforms, and are required to maintain multiple separate passwords, they can use a single, quality password, as defined above for all services;
- Do not send password over the network in clear-text, all passwords must be encrypted, this includes the delivery of initial passwords and/or password resets;
- Help desk personnel dealing with initial, lost or forgotten passwords will insure that only the intended recipient receives the new password.

In meeting this requirement, SVCC has adopted the following controls:

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.
- Users of MyVCCS and any related system are required to change their passwords after a period of 180 days.
Logical Access Control – *Password Management*

- 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
- 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.
- Easy to remember;
- Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
- Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
- Free of consecutive identical, all-numeric or all-alphabetic characters;

  - See [SVCC IT Security policies](#), policy 5.1.3, *Password Policy*
  - Also see, *Password Management* document, SVCC Security Plan section E 2. Location: Security\SVCC ISO 27002 2011\Phase II\SVCC Phase II\11 Access Control\E Logical Access Control\E 2 Password Management.

**Requirement:** *(Unattended user equipment - §11.3.2)*

Users will ensure that unattended equipment has appropriate protection.

All users will be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection as part of the security awareness training received.

During this training users will be advised to:
Logical Access Control – *Password Management*

- Terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
- Log-off mainframe computers, servers, and office PCs when the session is finished;
- Secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. hard disk encryption password access, when not in use.

Non-user specific equipment installed in user areas, e.g. kiosks, workstations or file servers, require specific protection from unauthorized access when left unattended for an extended period and will be hardened.

In meeting this requirement, SVCC has adopted the following controls:

- See [SVCC IT Security policies](#), policy 5.1.3, *Password Policy*.
- Location: Security\SVCC ISO 27002 2011\Phase II\SVCC Phase II\11 Access Control\E Logical Access Control\E 2 Password Management.
- See [SVCC IT Security policies](#), policy 7.1 Facilities Security.

**Requirement: (Secure log-on procedures - §11.5.1)**

Access to operating systems must be controlled through secure log on procedures. These procedures are designed to minimize the possibility of unauthorized access to Systems and data residing on these systems. These controls take into account:

In meeting this requirement, SVCC has adopted the following controls:

- Passwords entered by the user must not be displayed in readable format.
- Passwords entered into the systems must **not** be transmitted over the network in clear text (unencrypted) format; systems must encrypt the password information prior to transmitting them over the network to prevent network “sniffer” programs from capturing password information.

  - See [SVCC IT Security policies](#), policy 5.1.3, *Password Policy*. 
Logical Access Control – *Password Management*

- Also see, *Password Management* document, SVCC Security Plan section E 2. Location: Security\SVCC ISO 27002 2011\Phase II\SVCC Phase II\11 Access Control\E Logical Access Control\E 2 Password Management

**User identification and authentication (§11.5.2)**

All users of Systems Office and VCCS College data systems must be issued individual identifiers (user id’s) to log on to the systems. Users may not share their user ids with anyone, and suitable authentication techniques must be used to verify the identity of users.

In meeting this requirement, SVCC has adopted the following controls:

- See Requirements 11.2 and 11.3 above.
- Consider the use of strong authentication and identification techniques such as cryptographic, smart cards, tokens, or biometrics in addition to a password for systems that store data that is sensitive with respect to confidentiality or integrity.
  - See [SVCC IT Security policies](#), policy 5.1.3, *Password Policy*.

- Also see, *Password Management* document, SVCC Security Plan section E 2. Location: Security\SVCC ISO 27002 2011\Phase II\SVCC Phase II\11 Access Control\E Logical Access Control\E 2 Password Management

**Password management system (§11.5.3)**

Systems for managing Systems Office and VCCS College passwords should be interactive and should ensure that only quality passwords (as defined in the VCCS Password management standard) are used. The Systems Office and Colleges should:

In meeting this requirement, SVCC has adopted the following controls:

- See Requirements 11.2 and 11.3 above.
- Enforce the use of individual user IDs and passwords to maintain accountability;
- allow users to select and change their own passwords and include a confirmation procedure to ensure that no errors were made during entry;
- enforce the choice of secure passwords with password length, complexity, and change intervals;
- require users to change their initial passwords at first log-on;
Logical Access Control – *Password Management*

- Require that systems be configured to never display entered passwords on the screen; passwords should be hidden as they are entered into the system to avoid interception by others;
- Password files should reside on servers separate from the applications they are protecting, such as on an Active Directory domain controller;
- Stored passwords must be stored in encrypted format, never in clear text.

  o See [SVCC IT Security policies](#), policy 5.1.3, *Password Policy*.
  o Also see, *Password Management* document, SVCC Security Plan section E 2. Location: Security\SVCC ISO 27002 2011\Phase II\SVCC Phase II\11 Access Control\E Logical Access Control\E 2 Password Management

Session time-out (§11.5.5)

Operating systems should be configured to timeout inactive user sessions after a predefined time period. Inactive sessions increase the likelihood that unauthorized users could use the credentials of the logged on user to gain access to the system and data, or to cause denial of service to legitimate users. The Systems Office and Colleges should:

In meeting this requirement, SVCC has adopted the following controls:

- Implement an automatic session time-out after a period of time commensurate with the security risks of the area and of the sensitivity of the system data, but no more than after thirty (30) minutes of inactivity for systems with access to non-public information;
- Time out facilities should, at a minimum clear the session screen and implement a password protected screen saver and for higher risk areas and more sensitive data, consider closing both the application and the network session.

  o See [SVCC IT Security policies](#), policy 5.1.3, *Password Policy*.
  o Also see, *Password Management* document, SVCC Security Plan section E 2. Location: Security\SVCC ISO 27002 2011\Phase II\SVCC Phase II\11 Access Control\E Logical Access Control\E 2 Password Management