SCHOOL OF VISUAL ARTS

# 2025 SVA Password Standard

Version: 2026.03.11

Category: Network & Access Management

## STANDARD

### PASSWORD COMPLEXITY

Strong passwords are required for all accounts issued by SVA. All passwords, including initial/temporary passwords, should be constructed, implemented, and maintained according to the following guidelines:

Strong passwords contain a minimum length of (8) characters and are composed of at least three of the following characteristics (using all four is encouraged):

At least one numeric character (0-9)

At least one lower case character (a-z)

At least one upper case character (A-Z)

At least one non-alphanumeric character* (~, !, @, #, $, %, ^, &, *, (, ), -, =, +, ?, [, ], {, })

Note : Be advised that some systems may not support non-alphanumeric characters.

### STRONG PASSWORDS

When constructing a password, remembering these guidelines can increase its strength:

Do not use words in any language, slang, dialect, jargon, etc.

Do not use personal information such as names (relatives, pets, etc.), or dates such as birthdays or anniversaries.

Do not use words, phrases, or acronyms associated with the school (e.g., "sva")

Do not use computer terms, commands, sites, or software applications (e.g., "portal", "blackboard", "mysva")

Do not use word or number patterns (e.g., "aaabbb", "qwerty", "zyxwvuts", "123321", "abc123", etc.)

Do not increment previous passwords by prepending/appending additional characters ("password1", "1password", etc.)

## PASSWORD CHANGE FREQUENCY

Regularly changing passwords is a sound security principle that adds to the overall security of school's IT resources and systems. Depending on the classification of information particular passwords should be set to expire at regular intervals. Passwords for newly activated accounts must be changed on first use.

## PROTECTION OF PASSWORDS

All passwords must comply with the following:

Default passwords must be changed to conform to this best practice prior to deployment of all software applications, systems, and other IT devices on the SVA network.

System administrators must validate the identity of the user prior to performing a password reset on the user's account.

Users must never share or reveal passwords with or to anyone (e.g., supervisor, a spouse, child, or secretary). Shared accounts are thus prohibited.

Passwords must not be displayed, stored, or transmitted in plain text (e.g., authentication requests, unencrypted protocols, batch files, automatic log-in scripts, software macros, terminal function keys, devices without access control).

Passwords must not be stored in any location where unauthorized individuals might discover or obtain them.

If a user suspects their account has been compromised, the password on that account or system and all other accounts or systems using that same password must be changed immediately.

Other " Do not's " include:

Do not reveal a password to ANYONE

Do not reveal a password in an email message

Do not talk about a password in front of others

Do not hint at the format of a password (e.g., "my family name")

Do not reveal a password on questionnaires or security forms

Do not share a password with family members

Do not reveal a password to co-workers while on vacation

Do not write down your password and store it in plain view or in any other insecure location

Do not store passwords in a file on ANY computer system without encrypting the file

As a general rule, there are no legitimate reasons that a password should be revealed by any method to any person. The only notable exception to this rule is a situation where a user is being assisted in person by a known and trusted SVA IT support technician. After assistance has been rendered, the user should immediately change the shared password. Social engineering attacks generally rely on a user's trust of IT support personnel to obtain passwords.

The Administrative & Network Services department will perform various password auditing, cracking, or guessing efforts on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change that password. If the same password is used to access other systems, it is recommended that the user change the password on all systems where it is used. All other unauthorized attempts to "break", "hack", "crack", or otherwise determine a user's password are prohibited.

## Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of SVA property (physical or intellectual) are suspected, SVA may report such activities to the applicable authorities.

## Definitions

N/A

## Revision History

This policy shall be subject to periodic review to ensure relevancy.

Date

Description of Change

Reviewer

8/1/2015

Rev 1.0

C. Tomescu

6/21/24

Rev 2.0 – Periodic review and update

C. Tomescu

6/1/20205

Rev 3.0 – Periodic review and update

C. Tomescu