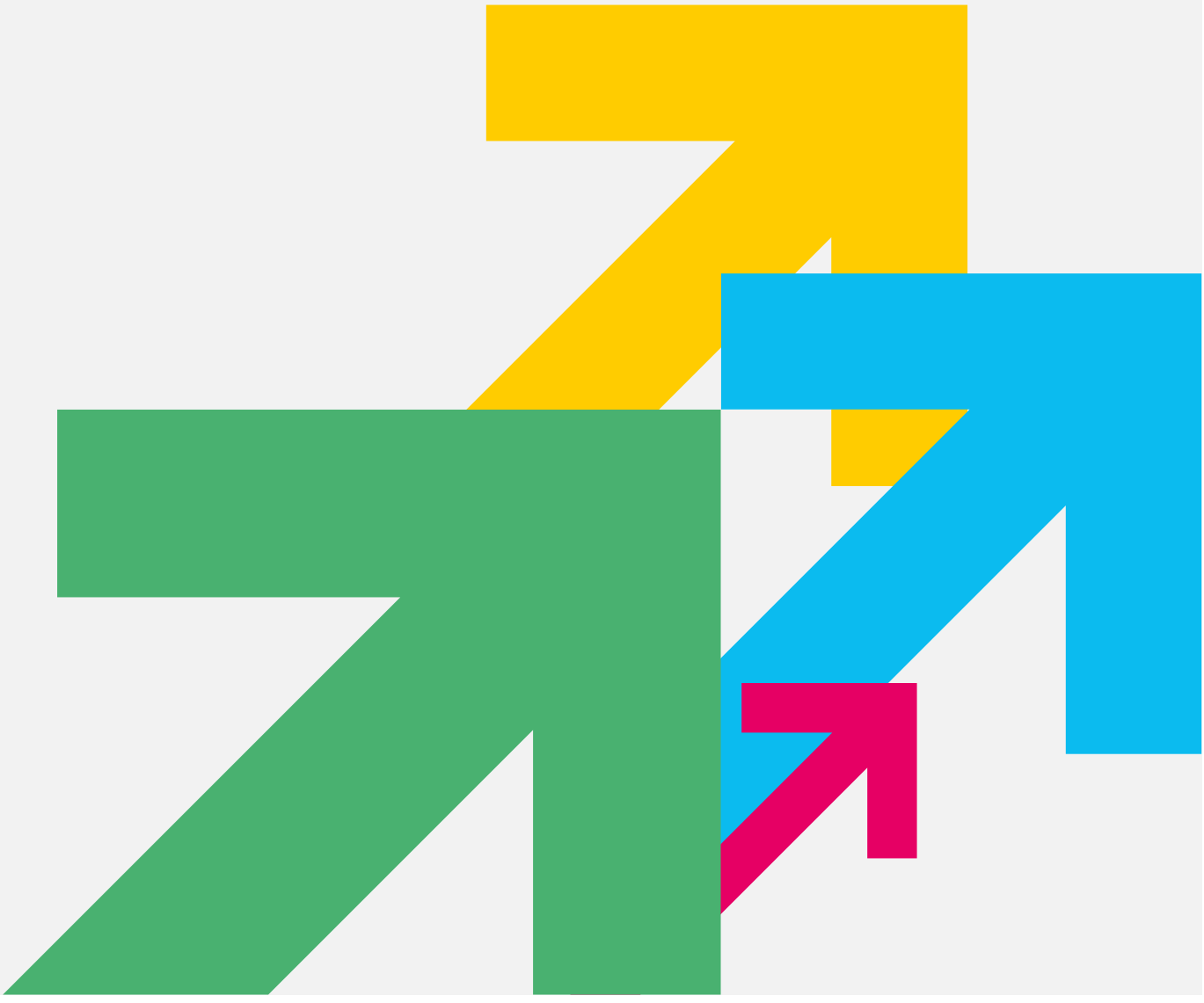
South Thames Colleges Group

IT Systems Password Policy

July 2023

RAD Volo



IT SYSTEMS PASSWORD POLICY

Purpose
The purpose of this policy is to establish a standard for the creation of very strong passwords, the protection of those passwords, and the frequency of change of the passwords for System Administrator and other privileged accounts.

Scope
The scope of this policy covers users who have responsibility for the Administration of IT Systems or Services within the College Group. This includes all users who have System Administrator and/or Sys Admin accounts. These users must change the password to their privilege account at least every 60-days.

Password Construction Guidelines
Passwords are used for various purposes, some of the more common uses include user level accounts, web accounts, email accounts, everyone should be aware of how to select complex passwords.

Complex Passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least 8 alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, etc
- Are not based on personal information, names of family, etc
- Passwords should never be written down or stored on-line

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:

    - Names of family, pets, friends, co-workers, fantasy characters, etc
    - Computer terms and names, commands, sites, companies, hardware, software
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns like xxxyyy, qwerty, 123321, etc
    - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (e.g., Dell1, 1Dell)

Password Protection Standards

Do not share your passwords with anyone including IT Services. All passwords are to be treated as confidential information.

Here is a list of dont's:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to a senior member of staff
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members

- Don't reveal a password to co-workers while on vacation
- Do not write passwords down and store them anywhere in your office
- Do not store passwords in a file on ANY computer system (including mobile devices) without encryption
- If someone demands a password, refer them to this document or have them call someone in IT Services
- If an account or password is suspected to be compromised, report the incident to the Helpline IMMEDIATELY