Student Password Procedure

Purpose: The purpose of these Standards is to ensure a high level of security for local area networks serving CGTC sites by providing a mechanism for controlling and ensuring accountability for access to the local area network, attached resources, and the Internet via user authentication with a unique user ID and password.

Related Standards and Policies:
TCSG State Board Procedure 3.5.1p1.a1 – TCSG Information Security Standards

Definition of User ID/Password: The unique combination of login credentials that identifies a specific piece of equipment or individual user.

Definition of Two-step Verification or Two-step Authentication: The method of requiring the users to confirm their identity by utilizing something they know, like a password, and then utilizing some sort of out-of-band mechanism like a one-time-password generator, security question, Authenticator App on their phone, SMS message, or Campus location.

Definition of Passphrase: Passphrases are defined as being a phrase, sentence or other group of words used in place of a standard password.

Procedure:

1. Any device that allows a user to connect to the campus network is a point of network access. To prevent unauthorized access, a user ID and password must be used to protect all points of network access.
2. The combination of Passwords and User IDs are confidential and must be protected. Sharing login credentials or logging on using another user's credentials is prohibited.
3. The maximum password life for CGTC students is 180 days.
4. Passwords may be assigned to users by the College ISA or his/her designee.
5. Initial passwords or password changes by the College ISA or his/her designee should require a password change on the first login. If there is a technical option that will perform this operation, it is preferred over relying on the user to change the password.
6. All passwords are required to adhere to the following rules, subject to operating system/application limitations:
   a. It is recommended that all student users have Two-Step or Multi-factor Authentication enabled.
   b. 8-character minimum and must include 3 of the 4 following items:
      i. Upper case: A-Z

        ii. Lower case: a-z

        iii. Numbers: 0-9

        iv. Special characters: ~!@#$%^&*()_+=-{}[]`|?><,.;

    c. Initial password must be unique and not contain the college name.

7. The College Information Security Administrators shall develop a procedure to remove accounts that are no longer required.

8. Students who have never attended will have their accounts removed after 365 days.

9. Students who have registered and attended at least one class but no longer registered after 365 days will have accounts limited to email and student information system access only.

10. The College Information Security Administrator, as defined in ISS-00, is ultimately responsible for implementing password standards. TCSG and the College ISA have the authority to permit or deny any user access to network and network-attached resources.

11. These standards represent minimum requirements. Users are encouraged to use more complex passwords and passphrases and to change passwords more frequently. Use of passphrases or the first characters of words in phrases are encouraged. Substitution of special characters for letters in the body of the password is encouraged. When possible, the use of non-ASCII standard characters is encouraged.

12. These standards will be reviewed periodically and revised based on changing information security requirements.