PROCEDURE: 3.3.4p.L.3
WGTC Student Account and Password Procedure
Adopted: February 24, 2020
Revised: June 30, 2022

Overview

Passwords are an important aspect of computer and network security. They are the front line of protection for user accounts, domain assets, data systems, and other technology resources. A poorly chosen or compromised password may result in a compromise of Wiregrass Georgia Technical College (WGTC) Student's network and private data. As such, all WGTC students are responsible for taking the appropriate steps, as outlined below, to select, secure, and maintain their credentials.

Purpose

The purpose of this procedure is to establish a standard that adheres to TCSG IT Security Guidelines for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

Students are assigned a WGTC domain account at the time of onboarding and acceptance into the college. Acceptance is defined as a student meeting all requirements for enrollment into a college program, dual enrollment, or for other official college business. The domain account consists of one identification credential (username) and one authentication credential (password). The credentials will allow the user to access many services on the WGTC **student.wiregrass.edu** Domain, as needed and authorized. For the complete list of available services, see Appendix A.

Procedure

Password Guidelines

WGTC Information Technology Department enforces the use of strong passwords, currently defined as:

- Must be at least 8 (eight) characters long and must include 3 of the 4 following items:
  - At least one upper case letter.
  - At least one lower case letter.
  - At least one number.
  - At least one special character.
- In addition, it cannot contain your first or last name.

See Appendix B for strong and weak password examples.

Multi-factor Authentication
Multi-factor Authentication will be used through Okta, both on the school network as well outside the school network. Anytime a user accesses email or other O365 products from a new or untrusted device, or changes his/her password, Okta will require that the user also authenticate through text message, phone call, or Okta Verify App. These preferences will have to be set up through the settings section for each individual account in Okta.

Account Deletion
All accounts will be disabled after two subsequent years of non-enrollment in classes, or as a result of account misuse, fraud, or dismissal from WGTC.

Password Protection Standards
Users will not share WGTC passwords with anyone, including other students, faculty, or staff of WGTC. All passwords are to be treated as sensitive, confidential WGTC information. There will be situations when a user will need to provide an existing or proposed account password to the WGTC IT Department. Otherwise, to best protect your password, please adhere to the following:

- Do not reveal a password over the phone to anyone.
- Do not reveal a password in an unencrypted email message.
- Do not share your password with anyone, including other students or faculty/staff of WGTC.
- Do not hint at the format of a password.
- Do not reveal a password on questionnaires or security forms.
- Do not leave a password with anyone while on vacation.
- Do not write down and store passwords anywhere.
- Do not store passwords in a file on ANY computer system in an unencrypted format.

If someone demands your password, refer him or her to this document and/or have them contact the Chief Information Officer or ithelpdesk@wiregrass.edu, then change the password immediately. If an account or password is suspected to have been compromised, immediately report the incident to ithelpdesk@wiregrass.edu.

Penalties
Any student found to have violated this procedure may be subject to disciplinary action, up to and including expulsion from the college per the TCSG Student Discipline Procedure.

Responsibility
The Chief Information Officer has the overall responsibility of ensuring this procedure is implemented.

References
TCSG 3.3.4p Procedure – Acceptable Computer and Internet Use.
National Institute of Standards and Technology (NIST) Special Publication 800-63B
https://pages.nist.gov/800-63-3/sp800-63b.html

TCSG Information Security Standards
3.3.4p.a1 Procedure - User ID and Password Standards (ISS-03)
https://it-http.tcsg.edu/TCSG-ISS/ISS-03%20-%20USER%20ID%20AND%20PASSWORD%20STANDARDS.pdf

Appendix A

List of domain resources available with WGTC wiregrass.edu account. WGTC currently uses Same Sign-On for access to the following:

- WGTC computer systems and servers, as authorized.
- Microsoft O365 and Email Portal.
- WGTC Blackboard Learning Management System.
- Banner Student Self-service Navigator (BannerWeb), as authorized.
- Banner Mobile App, as authorized.
- EAB (Educational Advisory Board) Navigate, as authorized.
- CampusLogic (Financial Aid Onboarding), as authorized.

Appendix B

Strong and weak password examples:

Strong password examples

- 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 eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, names of pets, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Poor, weak password examples – Avoid these mistakes in your passwords

- 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.
- The words "<Company Name>", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)