PROCEDURE: 3.3.4.p.L.2
WGTC Account and Password Procedure
Adopted: February 24, 2020
Revised: June 30, 2022

Purpose

Wiregrass Georgia Technical College (WGTC) is accredited by the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC). WGTC provides SACSCOC access to its operations and complete and accurate information about the college's affairs, including reports of other accrediting, licensing, and auditing agencies. The purpose of this procedure is to establish a standard that adheres to Technical College System of Georgia (TCSG) IT Security Guidelines for the creation of email accounts, strong passwords, the protection of those passwords, and the frequency of change.

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 password may result in a compromise of Wiregrass Georgia Technical College's (WGTC) network and private data. As such, all WGTC employees, including contractors and vendors with access to WGTC systems, are responsible for taking the appropriate steps, as outlined below, to select, secure, and maintain their credentials.

Scope

Faculty, staff, contractors, auditors, and vendors are assigned a WGTC domain account as needed, and upon onboarding with the college. 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 wiregrass.edu Domain, as authorized by supervisors and data owners. 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 14 (fourteen) characters long.
- Must contain at least one upper case letter.
- Must contain at least one lower case letter.
- Must contain at least one number.
- Must contain at least one symbol.
- Cannot contain your first or last name.
- Cannot be one of the past 5 (five) passwords used.

- Expire within a maximum of 45 calendar days.

Accounts with Global Domain Administrator privileges must have passwords that are at least 16 (sixteen) characters in length, cannot be one of the past 10 (ten) passwords used, and adhere to all other requirements. Other accounts with escalated privileges may receive more stringent password requirements as deemed necessary.

Administrator and Root account passwords will be changed annually at the beginning of the fiscal year (July), or whenever a staff member known to possess those credentials leaves or transfers.

See Appendix B for strong and weak password examples.

Multi-factor Authentication

Multi-factor Authentication (aka Okta) will be used, both on the school network as well as 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 Creation

Faculty, staff, contractors, auditors, and vendors are assigned a WGTC domain account as needed, and upon onboarding with the college. The account creation process for Wiregrass employees consists of the following steps:

1. HR contacts new hire with employment offer and instructions;
2. New hire completes all paperwork and submits it back to HR;
3. HR notifies IT of the new hire and provides account details (i.e. first name, last name, campus, department, job title, etc.);
4. IT creates the new hire's email address and temporary password;
5. New hire receives email address and temporary password from IT and/or supervisor.

WGTC employee domain accounts are typically created using the following format: *legalfirstname.legallastname@wiregrass.edu*. During the account creation process, the legal first name is used within the email address unless a preferred name was provided during the onboarding process. Once an employee account has been created, name changes are only allowed in the event of a marriage or divorce. Name change requests must be submitted through the HR Department.

Account Deletion

All accounts will be disabled at the time of the user's exit interview, resignation, release, dismissal, retirement, or other designated point in time and should be **coordinated in advance with the WGTC IT Department.** Emails will automatically be forwarded to a supervisor or designated recipient for 30 days, unless reasonable justification is provided and approved to extend this period. After the 30-day or approved period, the account will be terminated automatically.

Password Protection Standards

Users will not share WGTC passwords with anyone, including administrative assistants or supervisors. 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 a password with colleagues or supervisors.
- Do not hint at the format of a password.
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not leave a password with anyone while on vacation.
- Do not use the "Remember Password" feature of applications.
- 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, report the incident to the Chief Information Officer or ithelpdesk@wiregrass.edu.

Penalties

Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment and/or prosecution to the full extent of the law.

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 Single Sign-On for access to the following:

- WGTC computer systems and servers, as authorized.
- WGTC Email and Webmail Portal (Microsoft).
- WGTC Blackboard Learning Management System.
- WGTC Sharepoint and O365 applications (Microsoft).
- Banner Application Navigator, as authorized.
- Banner Student and Faculty Self-Service (BannerWeb), as authorized.
- Banner Mobile App, as authorized.
- EAB (Educational Advisory Board) Navigate, as authorized.
- EAB Campus, as authorized.
- WGTC Assist modules, as authorized.
- WGTC IT Self-service and help desk portal.

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 14 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)