Policy Source: Gwinnett Tech	Owner: Executive Director, IT	Effective: 3/2002
Division: Technology & Operations	Reviewed: 6/05, 2/2010, 3/2019, 12/2020 Revised:	

7.2.7 GT User ID and Password Guidelines

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

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

1. Any device which allows a user to connect to the Campus network is defined as a point of network access. All points of network access must be protected by a userID and password to prevent unauthorized network access.

2. The creation standard for non-student userIDs is as follows: First initial full last name, if duplicate userIds result then add middle initial following first initial. No nonalphanumeric characters allowed in usernames.
   Example: Mike Peterson = mpeterson
   Mary Lyn Peterson = mlpeterson (if mpeterson already in use)

3. Use of generic (multiple users using same userID/password) logins (userid/password combinations) is greatly discouraged, as accountability and audit ability are severely compromised. Generic logins may only be used for specific, limited time applications, and distribution of the login credentials will be limited to persons authorized for specific applications.

4. Passwords/user IDs are confidential and must be protected. Sharing of login credentials or logging on using another user's login credentials is prohibited and my result in disciplinary action.

5. UserIDs will be disabled after 5 invalid password attempts. Administrator intervention and review is required for re-enablement of password. (No automatic resets)
6. All passwords are required to adhere to the following rules, subject to operating system/application limitations (ie aix/oracle/mac-os)

   8 Characters Minimum and must include
   Upper case: A-Z

Lower case:	a-z
Numbers	0-9

No password (regardless of level) may contain:

	Examples
Single dictionary words:	dolphins
Proper names:	Mary1234
The userID associated with that account:	msmith12
Repeating characters	xxxx0000

No password may be less than 8 characters in length.

7. 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.

8. TCSG approved and trained Information Security Administrator for College is ultimately responsible implementation and enforcement of password guidelines. TCSG and the College ISA have authority to permit or deny any user access to network and network attached resources.

9. These guidelines are MINIMUM requirements. Users are encouraged to use the most lengthy and complex passwords possible and to change their passwords frequently. Use of pass phrases 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, use of non-ascii standard characters is encouraged.

10. Periodic security audits will be performed by College ISA and TCSG personnel using appropriate tool sets to assure compliance with stated information security policies. User accounts found not to be in compliance may be disabled until proper passwords are implemented or assigned.

11. These guidelines will be revised based on changing information security requirements.