Password Policy

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the Gadsden State Community College network. This policy provides guidance for creating secure passwords.

2. Purpose

The purpose of this policy is to provide acceptable practices for the creation of strong passwords.

3. Password Requirements

Passwords should be changed periodically. GSCC passwords are required to be changed every 180 days.

Changed passwords must significantly differ from a previous password.

All passwords should meet or exceed the following guidelines. These requirements are enforced by electronic policy.

Strong passwords have the following characteristics:

- Must differ from your previous password.
- Must include at least one number, one lower case letter, and one uppercase letter.
- May not be the same as the username.
- Must be 8 characters or longer.
- Must not be a simple password such as “Password1”.

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary or are common slang
- Contain personal information such as birthdates, addresses, phone numbers, or names
- Contain work-related information such as building names Contain number patterns such as aaabbb, qwerty, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).

You should never write down a password. Instead, you should use an encrypted, secure password manager such as KeePass.

(NOTE: Do not use any of these examples as passwords!)

4. Policy Compliance

4.1 Compliance

The Systems Administrator - Cybersecurity will verify compliance to this policy through review of electronic policy and implement appropriate electronic policies to ensure compliance.

4.2 Exceptions

Any exception to the policy must be approved by the Chief Information Officer.

Student Password Reset Policy

Overview

Gadsden State Community College students, faculty and staff who forget their user account password can use the Reset Password link located on the my.gadsdenstate.edu portal to reset their password online quickly and securely. An individual must have previously selected online security questions, recovery email, or recovery phone number before using the Reset Password link to reset a password. If a user of an account forgets their password, they will be prompted to answer these security questions in order to verify their identity. If a user of an account forgets their password and they have not set their security questions, they will need to enter a help desk request to have their password reset.

Purpose

The purpose of this policy is to define when it is acceptable for the help desk staff to reset student passwords.

Password Resets

The help desk staff are authorized to reset passwords only after confirming that the individual requesting the reset is the account owner. Exceptions to mitigate information security concerns may be authorized by the CIO or a member of the ITS InfoSec group. Requests from parents, faculty or staff to reset forgotten student passwords cannot be approved.

Policy Compliance

The Chief Information Officer will verify compliance to this policy through review of help desk tickets and communication with the help desk staff. The Chief Information Officer must approve any exception to the policy.