Gordon State College

Password Security Policy

Revisions

Original Date: February 26, 2014

Revision Number	Description	Date	Revised By
1	Changed minimum password length from 8 to 10	8/28/2017	Troy Stout
2			
3			
4			
5			

Reviewed

Review Date	Reviewed By
2/26/2014	Troy Stout
1/15/2015	Troy Stout
9/22/2016	Troy Stout
8/28/2017	Troy Stout

Purpose

The rising frequency of security incidents involving network-attached devices significantly increases the probability that sensitive data, if not properly authenticated and protected, may be exposed to unauthorized viewing or modification. Addressing these security concerns has become an increasing concern of the institution. Password management is a key aspect of computer security and is the front line of protection for user accounts. This policy identifies the minimum password requirements, to the degree technically feasible, for any users, systems, applications, and devices to protect Gordon State College's data and computer systems. Adhering to password standards will help us to protect the confidentiality, integrity, and availability of all college information systems/resources.

Scope

These standards apply to all electronic devices and systems connected to the Gordon State College network. All Gordon State College administrators, faculty, staff, students, contractors, guests and any other individuals who use the College's information resources shall take appropriate steps to select and secure their passwords.

Standards

All systems and applications must follow the minimum requirements for passwords, through technology or practice, set forth below:

1. Passwords should never be written down or placed in plain view by others (i.e. PostIt Note on monitor), or stored in plain text online. Choose a password you can remember. If a password must be written down it must be stored in a secured location.
2. All user-level passwords must be changed every **122** days.
3. Passwords must have a minimum length of **ten (10)** alphanumeric characters. On systems with a maximum password length of less than 10 characters, system administrators will set password controls to use the maximum length that the system supports where possible.
4. Users must choose complex passwords that contain at least three out of the four categories of characters below:
    - At least 1 uppercase character
    - At least 1 lowercase characters
    - At least 1 base 10 digit
    - At least 1 symbol found on the keyboard (such as !, @, #)
5. Users can not choose any of their last **five (5)** previously used passwords. Users or administrators who have changed their password must not be allowed to change passwords immediately to prevent individuals from changing their passwords multiple times to get back to their old password.
6. Technology permitting, user accounts will become automatically locked after **five (5)** unsuccessful or failed logon attempts for duration of **five (5)** minutes.
7. Passwords should not contain all or part of the user's full name, username, birth date, social

security number, mother's name, dog's name or any other information that someone may know about you. Dictionary words and repetitive characters must also be avoided when choosing a password.

8. Any newly provisioned user accounts must be provided in a secure manner and passwords changed upon first logon.
9. Passwords must not be inserted into e-mail messages or other forms of electronic communication unless properly encrypted.
10. Users must prevent passwords from being known or used by others:
    - Users must log off of applications when done using them.
    - Users should secure workstations when they are away (e.g. perform a Windows Lock).
    - Users should not use the "Remember Password" feature of any systems or applications.
11. If an account or password is suspected of being compromised, reset the password immediately and report to the Computer Services office.
12. Users should create a different username and password from their Gordon State accounts for external services such as personal e-mail, online banking and stores, or other systems.
13. Vendor supplied default and/or blank passwords shall be immediately reset upon installation of the application, device, or operating system.

Privileged and Shared Group Accounts

All privileged accounts (root, super user, and administrator passwords for servers, databases, network devices and other systems) should adhere to the requirements listed above where possible and/or technically feasible. Passwords on critical and/or sensitive IT systems must be changed, at a minimum, every **ninety (90)** days.

In situations where group or shared accounts for administrative purposes is required, the password must be changed immediately upon any personnel change within the group.