Password Strength and Security Standards

Information Technology: Policy IT-03
Effective Date: 11/10/17
Last Revision Date: 10/01/19

Contents

Per Grayson College's Password Policy, these Standards are required for passwords that provide access to College restricted data, or where otherwise required by law, GC or campus policy, or contract. They are recommended as good practices to follow for all passwords even where not required.

I. Introduction

Passwords are an important part of computer security at Grayson College. They often serve as the first line of defense in preventing unauthorized access to campus computers and data. Because of this, it is important to choose passwords that are complex and cryptic enough to prevent others from guessing them or from cracking them with “password cracker” programs. It is also important to keep passwords secret and secure so others can’t use them or find them.

These Standards are intended to provide information and guidance about how to create good, cryptic passwords and how to keep them secure and confidential. Some of the steps may require additional configuration/setting changes.

II. Password Strength Standards - How to create good, cryptic, hard-to-guess-or-crack passwords

REQUIREMENTS
The following requirements are enforced on many GC systems. Passwords that do not meet these requirements or are otherwise found vulnerable by automatic password strength checkers may be rejected.

1. **Passwords must be at least 8 characters in length and must contain 3 of the 4 following requirements:**
   - Lower case letters (i.e. a-z)

- Upper case letters (i.e. A-Z)
- Numbers (i.e. 0-9)
- Special characters (example: ! @ # $ %, etc)

2. **Passwords for systems or applications that cannot support the above standard must be longer -- at least 10 characters in length, if possible -- and incorporate the maximum complexity the system or application can support.**
3. **In addition, passwords must:**
    - Not be a single word found in the dictionary (in any language), whether spelled forwards or backwards, or a single word preceded or followed by a digit (e.g., secret1, 1secret)
        - Note: It is OK to use real words in passwords as long as you use more than one and still include the different required character types. Modified dictionary words are even better. See "Additional Tips and Hints" below for details.
    - Not include username, first name, or last name
    - Not be a common keyboard sequence, such as "qwerty89" or "abc123"
    - Not be from examples you have seen in print, such as the ones on this page
    - Not be a password you have used in the past

ADDITIONAL TIPS AND HINTS
for creating good, cryptic, hard-to-guess passwords

- Longer passwords are better.
- Avoid including personal information, names of family, places, pets, birthdays, address, hobbies, license plate number, etc.
- Avoid words that are slang, dialect, jargon, etc.
    - Basing your password on a phrase that is familiar to you is one way to generate a password that is memorable to you, but obscure to others. For example, "The hills are alive with the sound of music!!" is actually a pretty good password, except for the fact that that it is inconveniently long and published here. A shorter version could be, “HillsAliveMusic!” or, using a variant on the first letter of each word, "ThRawts0m!".
    - A few memorable, unrelated words can also be a good password, such as "HorseBattery" or, if the system requires additional complexity, “Horse!Battery!”
    - Automatic "password cracker" programs now also check for complete dictionary words in a row, separated by spaces or not, so it's still always best to modify dictionary words. "The hills are alyve w/the sound of musyc!" is much more secure than "The hills are alive with the sound of music!" It's also harder to remember, so it's a trade-off.
- Be aware that automatic "password cracker" programs check for common symbol substitutions in words, such as "0" for "o" and "$" for "s". Simply substituting

common symbols for letters in a dictionary word, e.g. "Pa$$w0rd" instead of "Password," might result in a guessable password even though it technically meets the above requirements. Passwords that are found vulnerable by automatic password strength checkers may be rejected.

- Passwords shouldn't be *too* common (Password1 is *very* common. 2bor!2b is pretty common and is also only 7 characters in length).

III. Password Security Standards - How to keep your passwords secret and secure:

1. **Do not share your passwords with anyone else, or in any way publish them.**

2. **Avoid writing passwords down.**

- Whenever possible, change passwords to something you can easily remember.
  - One way to do this is to create a password from a familiar phrase (see Additional Tips and Hints, above, for more information).
  - Once you have a good, strong, memorable password, you can come up with a system to modify it slightly for each system or application. Then you only have to remember your base password and your system.
- If you have to write a password down, try to write it in a way that others won't be able to decipher -- such as using a hint for part of it -- and store it securely in a safe, unlikely-to-be-discovered location, e.g., not under the keyboard or on your monitor.

3. **If you think your password may have been compromised, notify the IT department and your supervisor.**

4. **Change passwords provided for initial access or password resets as soon as possible.** Information for doing this should be provided with the password. If it is not, contact the person or office issuing the password for instructions.

Staff Password Change Instructions: Use the keyboard command **Ctrl Alt Del** from any campus networked computer or use the following instructions.

Faculty & Staff Password Change Instructions:

- Go to: https://www.grayson.edu
- Click on “MyViking”
- Click on “Forgot My Password”
  - Note: Username is not an email address

5. **Don’t let your applications or browser remember/store passwords that provide access to restricted systems or data.**

- That way if someone gets access to your computer, they don't also get access to all of your accounts.

6. **Use different passwords for accounts that provide access to restricted data than for your less-sensitive or personal accounts.**

- For additional security, use a different password for each account that provides access to sensitive data; that way if one of your passwords is compromised, your others are still OK.

7. **Ensure that passwords are transmitted securely.**

- Before you log into something via the web, look for "https" (not http) in the URL to indicate that there is a secure connection. If this is missing, request a secure web page from the service provider that you can use to log in.

IV. Getting Help

- Staff can use ***Ctrl Alt Del*** to change their password at any computer on the Grayson College network or use the following steps:

- Password change instructions for faculty, staff, and students:

- Go to: https://www.grayson.edu
- Click on "MyViking"
- Click on "Forgot My Password"
    - Note: Username is not an email address

- Contact the IT Dept with questions or feedback about these Standards, or to report a compromised password: http://help.grayson.edu

---