Complex Password Requirements

All Sinclair network accounts, including those for students, staff, and faculty, need to be protected from compromise and misuse. The “Key” to account protection is an effective password, and password *complexity* is a basic requirement of all effective passwords.

Please review the table below containing the following password requirements that will be automatically enforced:

Passwords Must NOT:	Passwords Must:
▪ Contain the user's account name ▪ Contain the user’s first name or the user’s last name ▪ Be the same as your previous 13 passwords	▪ Be at least **eight (8)** characters in length ▪ Contain characters from **three (3)** of the following four categories: ○ English uppercase characters (A through Z) ○ English lowercase characters (a through z) ○ Numbers (0 through 9) ○ Non-alphabetic (special) characters such as $ or ! (Important! Do **NOT** use any of the following: **": “; * : ' ”**)

NOTE: All campus users are required to change their network passwords every ninety (90) days.

Remember that a complex password doesn’t have to mean a hard-to-remember password. Some steps for creating a complex but easy-to-remember password include:

1. **Create a base word** - Pick a long ago fact or thing that's easy for you to remember but not necessarily easy for a hacker to know. For example, say you once lived in Timbuktu. Use that word to establish the base of your password.

2. **Add more characters to the base word** – add the required characters and mixed upper and lower case letters listed in the second column of the table above to the base word.

   An example of a strong password is: **59Timbuktu!**

Another very effective method for creating a complex password is to **base it on a sentence or statement you can easily remember.** For example, using the sentence I like to watch Dragons baseball games and some simple substitution results in the effective password

IL2wD$bg

(I Like 2 watch Dragon$ baseball games)

These new complex password requirements will take effect immediately for all new network accounts and for all existing network accounts.

In our college environment, federal and state laws—most notably FERPA—dictate how we handle much of the information we use. Who can access information, how this information can be used, and what standards or controls must be implemented are all part of the information security equation. Since the password is a primary protection method, it is imperative that every UserID is protected by a complex password to help ensure that Sinclair is in accordance with all applicable information laws and regulations.

Complex passwords are not meant to restrict or hamper campus PC activity but to protect user PCs and the college network. Complex passwords are important in fighting information breaches and can help the College avoid situations such as:

- System shutdowns
- Identity theft of students and employees
- Legal risks associated with data breaches

Complex passwords are the main protection from hackers and help to prevent them from easily guessing passwords and impersonating users thereby helping prevent the loss, exposure, or corruption of sensitive information.

NOTE: Your account will be locked after 10 failed login attempts in a 15 minute period. After 15 minutes, your account will automatically be unlocked.

NOTE: This does not affect Colleague passwords for faculty and staff.

NOTE: It is also recommended that you use complex passwords for your home use.

Some additional measures for protecting the security of your account's password and also at home include:

- Never store your password where anyone else can see it. Don't write your password on a post-it note and attach it to your monitor
- Change your password regularly
- Immediately change your password if you suspect that it has been compromised
- Don't share or loan out your password to other users
- Never provide your password to unsolicited requests such as what looks like an email from your bank or other businesses. These are often phishing techniques where hackers send emails that look like they are coming from your bank or other legitmate source etc. Sinclair will never email users asking them for their passwords.

Additional password security tips are found in this article:

http://it.sinclair.edu/index.cfm/information-security/securityawareness/tips-for-creating-effective-passwords/

Below is additional information from Microsoft about creating strong passwords:

Strong passwords help prevent unauthorized people from accessing files, programs, and other resources, and should be difficult to guess or crack. A good password:

o Is at least eight characters long
o Doesn't contain your user name, real name, or company name o Doesn't contain a complete word
o Is significantly different from previous passwords o Contains uppercase letters, lowercase letters, numbers, and symbols

If you believe your Sinclair password has been compromised or you have reason to believe it is no longer secret, contact the IT Help Desk and change your passwords immediately.

For questions or additional information, contact the IT Help Desk at 937-512-HELP (4357) or at helpdesk@sinclair.edu