

Guidelines for Managing Strong Passwords

Many users in the School of Medicine have accounts on several systems in the School of Medicine as well as on main campus and in the hospital. Most of those systems have password policies requiring strong passwords which must be changed every 90 days or less. Remembering numerous frequently changing passwords can be difficult and may encourage users to write them down, thereby increasing the possibility of compromise. The purpose of this document is to provide some guidelines for creating and managing strong passwords which are easy to remember.

Reduce the number of passwords to remember. If you have fewer passwords to deal with, then it should be easier to remember them and you should be less likely to write them down. However, it is not recommended that you use the same password on every system that you log into. It is recommended that you maintain at least three different passwords:

- **Work/school password** – Use the same password for all of the systems that you access on campus. This is a trade off between convenience and security. When using a single password, if the password is compromised, access is gained to all of the systems. However, with a single password, the user is less likely to write it down, decreasing the overall risk of compromise.
- **Personal password** –For all of your personal accounts, such as bank account access, private e-mail accounts, etc., use a password that is different from your work/school password.
- **“Junk” password** – Use a third password for all of the miscellaneous accounts that you are asked to create to get access to various commercial web sites. Passwords of this type are being supplied to third parties whose security practices and integrity are unknown. Work/school and personal financial passwords should never be used at these sites.

Change the passwords on all of your accounts at the same time. This practice reduces the confusion as to when different passwords may expire.

Create a strong password that is easy to remember. There are many techniques that can be used to create strong passwords which are easy to remember, yet are still secure. One example is provided in the following steps. For additional security, users are encouraged to vary these steps slightly. You should not use the specific examples below for your own passwords. The steps may seem confusing at first, but once understood, they can actually simplify remembering strong passwords.

Step 1. Think of a phrase you will not forget. Example: *Strong Security*.

Step 2. Take the first and last letter of each word in the phrase. Example (Strong Security from above): *Sgsy*

Step 3. Consider doing some of the following substitutions:

- a. All "e"s are changed to 3
- b. All "i"s are changed to 1

- c. All "o"s are changed to 0
- d. All "a"s are changed to @
- e. All "s"s are changed to 5

For our example this yields: **5g5y**

- Step 4.** Add a sequence string or number at the beginning or end. For example, if you change your password in January, add "Ja" or "1" for first month. From our example from above, we could now have: **5g5yJa**
- Step 5.** Add some special characters. Example: Use a "#" every few characters. For our example that we are building, we now have: **#5g5y#Ja#**
- Step 6.** Vary the sequence string each time you change passwords. For example, if you used "Ja" when you changed passwords in January, then maybe use "Ap" when you change passwords in April. For our example, our new password would become: **#5g5y#Ap#**