UNIVERSITY OF FLORIDA UF HSC SPICE The Focus is on YOU
Security Program for the Information and Computing Environment
http://security.health.ufl.edu

SPICE EduGuide EG0012
User Password Security

This SPICE EduGuide applies to users of the HSC computing environment, for example HSC workstations, servers, network, applications, and databases. Users of the HSC computing environment will be issued computer 'accounts' which are basically logon ids and passwords. Computer accounts are unique to each user, and help to ensure that the user logging in is able to access only what he or she is authorized by their supervisor to have. Computer accounts, particularly passwords, must be secured.

> **Compromise/Data Theft –** Computer hackers constantly seek access to computers and data that have no password protection, or that have passwords that are easily guessed. They employ 'password crackers' that automatically repeat a logon process using a set of predictable passwords (dictionary words, dates, etc.), until a successful login takes place. Hackers seek access for purposes such as data theft or illegal distribution of copyright material.
>
> **Masked Accountability** – Your shared or otherwise unprotected password could be used by a work associate with intentions of inappropriate access. User activity is monitored and logged (electronically recorded) and serious consequences apply to inappropriate access to **Restricted** information. The inappropriate access of another person who has learned and used your password, will appear in computer logs as *your* computer activity.

Safeguard Requirements and Guidance

- Keep your passwords secret. Do not share them with anyone, not even IT support staff or family members. A 'proxy' feature may be available in your applications to enable access sharing in an authorized manner. Contact the IT service providers of your applications to inquire about the availability of proxy access.
- Expect your computer systems to prompt you to change your passwords on a periodic basis. This period could vary from every 90 days to annually, depending on what you have access to.
- If you believe your password has been learned by someone else, don't wait for a periodic change. Initiate the change yourself and notify your Unit ISM. Computer systems should have a password change feature available to users.
- A UF or HSC computer system may reject a password you select if it does not meet the criteria for a 'strong' password. A strong password is one that is not easily guessed. The criteria for a strong password may change as the capabilities of hackers change. A password:
    - Should be at least eight characters long
    - Should not be a dictionary word, a name, your UF ID, your SSN, or a date
    - Should contain at least three out of these four elements — uppercase letters, lowercase letters, numbers, and punctuation/special characters.
- Memorize your passwords; if you must record them to remember them:
    - Never record them legibly in the same place; disguise or encrypt them
    - Do not post them on your monitor, keyboard, in desk drawers etc. Secure them the way you would secure a credit card.
- If your computer offers to "remember" your password, click NO.
- Do not use your work related passwords as the password for your personal computer accounts such as eBay or Yahoo.

Policy & Standards References:
TS0003 & TS0005 User Account and Password Management