This SPICE EduGuide applies to HSC information systems, specifically 'Administrative' login accounts; (aka Admin accounts) and the faculty, staff and students who use them. Admin accounts are logon IDs and passwords that are assigned powerful privileges to be able to do anything that can be done to a computer. People who know the Admin account logon ID and password are typically called the Systems Administrator. The Systems Administrator of a computer has the ability to set up other user accounts, delete other user accounts, reset another user's password then use it, install programs, delete programs, create data files, copy or delete any data files including those that belong to others, make the system work, and break the system indefinitely. Because of the power afforded to people who are granted Admin accounts over computers and network systems, granting Admin accounts needs to be done with caution and control.

What are the Risks?

"You've Been Owned" – Acquiring the Admin account logon ID and password is like striking the mother lode for a computer hacker. Once the Admin account password has been learned, the hacker in effect has taken over ownership of the computer. Hackers sometimes show their prowess by changing the screen saver to read "You've Been Owned" or putting the phrase in a broadcast message. But as computer hacking is becoming more profitable, the more significant risks are:

- This "new owner" becomes capable of learning the passwords of all the users on your system or making a copy of the password database to his/her own computer where password cracking tools can be applied at the hacker's leisure.
- This "new owner" can set up your computer to store and distribute illegally acquired software, music and games.
- This "new owner" can use your computer to contact other computers in the HSC. And because the hacker looks like a legitimate HSC Systems Administrator, he/she can spread malicious software to those other computers, then "own" them too.
- This "new owner" can take copies of patient files, student files or pictures or any other data he/she finds interesting on the computer. There have been reports in the news about students who are hackers getting paid by other students to systematically fix their grades. In addition, names, date of birth, and social security numbers sell in the black market for anywhere between $5.00-$8.00 per record.
- This "new owner" can shut your system down in many different ways, make it unavailable to your users, or delete all your data. The hacker can do such damage that without a contingency plan for such an event, recovery is indefinite.

With the exception of shutting your computer down, the hacker can do these things without being noticed if the system is not set up to monitor for these nefarious activities – and many aren't. In addition, the hacker can do all of this without any fear of retribution, because he/she has learned the Admin account password and so appears as a legitimate Systems Administrator.

What makes learning Admin passwords easy?

A large volume of Admin accounts increases the chance that a computer hacker will learn a password. If a Unit is of the practice of setting up all users with Admin access to their end user

workstation, it is far more vulnerable than one that has controlled the proliferation of Admin accounts. Consider the notion of giving keys to everyone versus giving them to a select few.

An Admin account with a weak password or with a password that does not expire regularly increases the chance that a computer hacker will learn the password.

One Admin account and password that is shared among multiple people increases the chance that an unauthorized person will use the account to harm the system.

Key loggers recording key strokes and sending Admin password entries to a hacker occurs more often than we know. Key loggers are small software programs that are unknowingly downloaded by the user through their use of the internet, and proceed to record everything the user types on the keyboard. It is a growing problem.

Why are Admin accounts desired by end users?

In the past, end users were set up with Admin like privileges. This practice enabled end users to install their own software on their workstation when they wanted to, and to change computer settings and preferences to meet their needs without involving their IT support person. Current wisdom no longer supports this practice, but end users do not want to give up the independence they have enjoyed as computer users. Recognize also there are personal tasks users do with their computer that they will be prohibited from doing or that will become apparent to the IT staff who have Admin privileges.

Understanding user needs and committing to service levels can help users feel they will still be able to get their work done without Admin like privileges. Still, Unit leadership should be prepared to hear from users about their loss of privileges.

Who should hold Admin accounts?

Admin accounts may not be freely distributed. Unit leadership is empowered to establish its own authorization rules for Admin account access, however, they must not conflict with the SPICE policy. SPICE policy on access authorization requires Units to authorize access based on "…the individual's role and responsibilities and the classification of an Information Asset." If Unit leadership is proactive in determining the Admin account authorization rules and openly communicates them, conflicts can be avoided. Here are three recommended steps to making authorization rules for Admin accounts:

1. Identify the legitimate responsibilities that require Admin privileges. Some examples include:
    a. Setting and ensuring the security controls of a computer such as firewall, antivirus updates, OS patch process, encryption if required, etc.
    b. Adding, modifying, deleting users
    c. Fixing or rebuilding the computer when it breaks
    d. Eradicating hacker presence
    e. Installing software
    f. Executing poorly written software that technically requires Admin access to execute properly (although the Unit should be actively searching for a better written replacement product)

   g. Being accountable for disruption or damage due to misuse or carelessness of the Admin account
2. Next, Unit leadership should determine what roles in the Unit have the stated responsibilities; generally people performing technical support of the computers or who have security responsibility.
3. Finally, Unit leadership should identify the person or person(s) who will review the Admin account requests and approve or deny them based on the roles and responsibility criteria that have been established. The delegated authorizer of Admin accounts should be someone well acquainted with the significance of an Admin account, and whose authorization decisions will be supported by Unit leadership.

Guidelines for authorizing Administrative Accounts:

- End user accounts should be examined and Admin privileges should be removed.
- Software and database developers should not have Admin access to production servers or end user workstations. The need for software developers to have Admin access to their development environment may be necessary, but in such cases the development environment should not also be the production environment and the software developer must ensure that the proper security controls are implemented and maintained.
- IT staff whose job it is to operate Unit servers and support end user workstations will need Admin account privileges, but not necessarily all IT staff in a department. The IT manager or director must carefully determine who among their IT staff should have this level of trust and should not simply authorize everyone in their department.
- Some small HSC departments do not have dedicated IT staff or have very few IT (i.e. 1) resources. The IT support responsibilities that require Admin access are being performed by people with multiple roles in the department. These people performing IT support responsibilities will need Admin account privileges to perform their job, however, the person authorizing the access should ensure the employee has had technical security training for system administrators to reduce the probability of a costly mistake.
- Computer support student employees should not be authorized to have an Admin account to computers of other users, or to servers. If there needs to be exceptions, the person authorizing the student to have an Admin account should ensure the student has had formal (not co-worker) systems administration training pertinent to the system, and is well supervised. The student's Admin account must be suspended and terminated when the student leaves, and should not be re-used by the replacement.
- Laptop computers are often used differently from desktops, generating a possible need for a laptop user to have administrative access to his/her laptop. This is highly dependant on how the laptop is used, and how it is configured by the IT department. The ISM should evaluate the need for administrative access for the laptop user. If such access is needed, laptop users should be provided with two accounts: a user account with privileges that limit the damage that can be done to their laptop, and an Admin account with privileges that permit the user to self-support when they need to. The user should always use their user account when using their laptop, and only use their Admin account when they need to install new software or change restricted settings.

The Dean, Director or Department Chair approves the authorization rules. Unit needs and requirements vary, so Admin access authorization rules will vary by Unit. Two things that should remain constant, however are 1) Unit rules should support the restriction of Admin accounts versus the propagation of Admin accounts, and 2) anyone with an Admin account must have a legitimate reason, and convenience will never pass an audit as a legitimate reason.

Safeguard Requirements

By SPICE policy, Admin account holders are "…responsible and liable for all processes initiated from their account." The implications of this policy statement are significant given the amount of damage that can be done intentionally or unintentionally from an Admin account. Admin account holders must comply with the following Admin account safeguards to properly protect the information and systems to which the Admin account provides access.

- Admin accounts must only be granted to those who have a need based on their job responsibilities. Ease of use and access are not justifiable reasons to grant someone an Admin account.
- Staff with Admin account privileges must not circumvent the User Account and Password Management Policy for the sake of convenience for either themselves or other users.
- Admin account holders should use a separate account for system administration tasks from the one they use as a computer user. The Admin account holder should log out of their normal user account and log back in as an administrator to perform system administration tasks, or use the RunAs (Windows) or sudo (UNIX/Linux/MacOS) feature to run commands and tools requiring administrative access.
- Administrative passwords should never be used in auto logon or 'remember password' features provided by computer systems. Passwords should never be embedded in scripts or hard coded in computer programs. Rare exceptions apply, but must be approved by the Unit ISM.
- University and HSC SPICE policies require that system activity logs be able to uniquely identify its user. Therefore, accounts with Admin privileges must be unique for each user and must not be shared.
- Some operating systems come with a generic Admin account that often is needed to be used by more than one System Administrator to support the system (i.e. the UNIX super user or 'root' account.) In these cases, the System Administrators must use a process whereby their individual system administration activity records can be uniquely associated with each person, such as the 'sudo' command.
- Admin accounts must be protected as follows:
  - Must be at least 8 characters long; contain an upper case and lower case letter, a number and a special character.
  - Must expire and be changed at least every 90 days.
  - Must be different from all of the other accounts held by the person.
  - Must be protected by encryption when stored and transmitted.
- Every computer typically has a 'local administrator' account that is used to setup and configure it, and is often needed by IT support personnel to fix problems with a user's

computer. While it is common practice for a unit to use the same password for the local administrator account on all the computers they support, this is a very poor practice. If an attacker were to discover the administrator password to one of the unit's computers, they would then have access to all of the computers. Two best practices are:

- In a domain or other shared directory environment, IT personnel can log in with a network-based account that provides administrative access. Set the local administrator password to something completely random and unknown to anyone. Use the largest password accepted by the system.
- If network-based administrative access is not possible, create a unique administrative password for each computer, using an algorithm that a remote attacker could not guess, but would be simple for local support personnel. One way is to combine a secret component and concatenate some externally visible uniqueness, such as the property decal number, or a serial number. For example 'F8jk7!HC136105'. In that password, 'F8jk7!' is the secret part, which is known to the authorized personnel, and 'HC136105' is the property ID which is visible on the front of the computer and makes the password unique to that computer. The algorithmically generated portion must be changed after a support staff member who knows the algorithm separates from the department.

Units who cannot secure Admin accounts with these guidelines and safeguards should contact the UF HSC Security Office for alternative solutions such as network isolation.

Policy & Standards References:

Policy TS0005 User Account and Password Management

Standard TS0003 User Account and Password Management

Policy GP0003 Information Security General Provisions