GOALS

- To prevent misuse of administrator privileges
- To minimize the risk of exploitation of uncontrolled administrative privileges
- To prevent attackers from cracking passwords and gaining access to target machines and protected data.

1) Administrator Accounts and Passwords
    a) Each IT support group should inventory all administrative users and validate that each person with administrative privileges on desktops, laptops, and servers is authorized and his or her administrative password meets the established criteria for passwords.
    b) Before deploying any new devices in a networked environment, UCLA IT support groups should change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to passwords that meet UCLA Health Sciences minimum criteria for passwords.
    c) As is done for regular accounts, all administrative-level accounts should require password changes at a 90-day interval.
    d) IT support groups should ensure all service accounts have complex passwords. When possible, service account passwords should be changed on a periodic basis as is done for traditional and privileged user passwords.
    e) Passwords for all systems should be stored in a hashed or encrypted format. Files containing these hashed and encrypted passwords for use authentication should be readable only with super user privileges.
    f) Administrative access should be restricted based on defined roles within the organization. For example, “Workstation Admin,” should only be allowed access to workstations and laptops – not servers, databases, or web applications.
    g) Systems should be configured to generate a log entry and alert when an account is added to or removed from a domain administrators group. Reports should be run and reviewed on a regular basis to monitor changes to the domain administrators group.
    h) Where supported, two-factor authentication should be used for Administrative access.

2) Use of Administrator and Super User accounts
    a) IT Administrators should establish unique, different passwords for their administrator accounts and their non-administrative accounts.
    b) Administrator accounts should be used only for the system administration
activities and not for reading e-mail, composing documents, or surfing the Internet.

c) When possible, web proxies/web proxy settings should be implemented to prevent administrators from using their privileged accounts to access the web.

d) Administrators must access systems remotely using a fully logged and non-administrative account. Then once logged in to the machine without admin privileges, the administrator should then transition to administrative privileges using tools such as sudo on Linux/Unix, runas on Windows, and corresponding facilities for other platforms/systems. When possible, remote access directly to a machine should be blocked for administrator-level accounts. The only exceptions will be for those cases where the administrative task to be performed can only be done when logged in as the Administrator.

REFERENCES
HS Policy No. 9452, “User Accounts (Authorizing Access to Restricted Information; Passwords)

CONTACT
Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY
Created Date: July 12, 2016