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.

STANDARD

1) Administrator Accounts and Passwords
   a) Administrative access should be restricted based on defined roles within the organization. For example, a “Workstation Admin” should only be allowed access to workstations and laptops – not servers, databases, or web applications.
   b) Each IT support group should regularly inventory all administrative users and validate that each person with administrative privileges on desktops, laptops, and servers is authorized; that the specific privileges each person has are limited to job-related needs; and that the system enforces the UCLA Health Sciences minimum criteria for passwords as specified in HS 9452, User Accounts (Authorizing Access to Restricted Information; Passwords).
   c) All administrative-level accounts should require password changes at a 90-day interval.
   d) 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.
   e) Where supported, two-factor authentication should be used for Administrative access.
   f) Where supported, administrative-level accounts should be integrated with enterprise Active Directory (AD).
2) Service and Device Accounts and Passwords
   a) Before deploying any new devices in a networked environment, UCLA Health 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.
   b) IT support groups should ensure all service accounts have passwords that meet UCLA Health Sciences minimum criteria. When possible, service account passwords should be changed on a periodic basis as is done for privileged user passwords. Service account passwords should also be changed upon termination of people (including staff and vendors) who had access to that

account.

3) Use of Administrator and Super User accounts
   a) IT Administrators should establish unique, different passwords for each of their administrator and non-administrator accounts.
   b) Administrator accounts should be used only for 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. Once logged in to the machine without administrative 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.

EXCEPTIONS

Any exceptions from this standard must be approved by the UCLA Health Sciences Chief Information Security Officer.

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
Revised: October 16, 2020