STANDARD

This standard describes the required minimal security configuration for all network devices used in a production capacity at or on behalf of UCLA Health Sciences. All network devices connected to UCLA Health production networks must comply with this standard. Network devices that are isolated from production networks are not affected.

1) All network devices, including but not limited to, routers, switches, firewalls, VPN gateways, wireless controllers, wireless access points and other appliances must be managed by UCLA Health IT.
2) Network devices should be physically located in an access-controlled environment.
3) Network devices should be managed across network connections that are separated from the business use of the network, relying on separate VLANs or, when possible, on entirely different physical connections.
4) Dedicated, stripped-down and secure jump boxes should be used to launch management session for network devices.
5) Whenever possible, centralized authentication, encryption sessions and multi-factor authentication should be implemented for network device management.
6) UC Health IT shall develop network device hardening standards and secure configuration templates for each type of network infrastructure device in use at UCLA Health Sciences. Any deviations from the secure template should be documented and approved by the Chief Information Security Officer.
7) Rigorous configuration management and change control processes and tools should be in place to control, monitor, alert and validate any change to network device configuration.
8) The latest stable version of a network device's OS or firmware that contains critical security updates shall be installed as soon as possible, but not more than 30 days after the update being released from the vendor.
9) IPv6 should be disabled if not in use.

EXCEPTIONS

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

QUESTIONS

1) Contact Customer Care at 310-267**-CARE** (2273) for any network need you may have.

2) Contact IT Security (ITSecurityAll@mednet.ucla.edu) for any questions on configuring network devices.
3) If you have questions about this Standard, please contact the Office of Compliance Services – Information Security (InfoSecAll@mednet.ucla.edu)

REFERENCES

HS Policy No. 9457, "*Minimum Security Standards*"

"The CIS Critical Security Controls for Effective Cyber Defense, V6.0," CIS Center for Internet Security

CONTACT

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Created Date: June 3, 2019