STANDARD

UCLA Health IT shall comply with the following requirements:

1) Hardening Standards
   a) UCLA Health IT shall maintain hardening standards that are in compliance with UCLA Health Information Security policies and standards for each type of supported operating system to ensure configurations will be secure.
   b) To obtain copies of the current standards, please contact IT Security (ITSecurityAll@mednet.ucla.edu).

2) Standardized master images
   a) UCLA Health IT shall set up servers, workstations and laptops using standardized master images.
   b) Standardized master images for servers, workstations, and laptops used by UCLA Health shall be built in accordance with industry best practices and the Hardening Standards.
   c) Standard master images will be approved by the Technology and Security Architecture Standards Board.
   d) The master images shall be validated and refreshed on regular basis.
   e) The master images should be stored on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible.

2) Security Patch Management
   a) UCLA Health IT will develop procedures for device and application patching.
   b) All security patches and hot-fixes recommended by hardware vendors, software vendors, and UCLA Health IT must be installed as soon as possible, and no later than one month after their release. This applies to all services installed, even though those services may be temporarily or permanently disabled.
   c) For patches determined to be critical, the Chief Information Security Officer may set a shorter time period for mandatory patching.
   d) Devices and applications that cannot be kept up to date on patches must be located in isolated subnets with minimal connectivity to internal networks.

3) Vulnerability scanning
   a) UCLA Health IT will develop procedures for Vulnerability management.
   b) UCLA Health IT will perform credentialed vulnerability scans of all devices (internal and external) on UCLA Health networks monthly.
   c) All vulnerabilities with a Common Vulnerability Scoring System (CVSS) score or 4 or greater must be remediated within 90 days. For vulnerabilities deemed high risk by the Chief Information Security Officer, shorter remediation times may be required.

d) All new servers/network devices must be vulnerability scanned before go live. All vulnerabilities with a Nexpose Rapid 7 Vulnerability Score greater than 400 must be remediated before go live.
e) All new web applications must have web application vulnerability scans before going live. All critical, high and medium vulnerabilities must be remediated before go live.
f) Systems that cannot be patched must be located in isolated subnets.

4) Penetration testing
   a) UCLA Health IT shall engage external parties to perform annual penetration testing.

EXCEPTIONS

1) Owners of systems that cannot meet the hardening, standard image, and/or vulnerability remediation requirements may request exceptions from the UCLA Health Sciences Chief Information Security Officer or designee.
2) All exceptions must be documented.

QUESTIONS

1) For information on technical issues or to request copies of the UCLA Health IT procedures related to this Standard, please contact the IT Security team (ITSecurityAll@mednet.ucla.edu).
2) To request an exception, please contact the Chief Information Security Officer.
3) For questions on this Standard, please contact the Office of Compliance Services – Information Security (InfoSecAll@mednet.ucla.edu).

REFERENCES

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

CONTACT

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Created Date: May 18, 2019