LAC+USC MEDICAL CENTER POLICY

	Page 1	Of 3
Subject: **IT SECURITY VULNERABILITY SCANNING AND REMEDIATION**	Original Issue Date: 2/11/14	Policy # **461.1**
	Supersedes: 9/22/17	Effective Date: 10/30/20

Departments Consulted:	Reviewed & Approved by:	Approved by:
Information Systems Office of Risk Management Office of Human Resources	Attending Staff Association Executive Committee Senior Executive Council	(Signature on File) Chief Medical Officer (Signature on File) Chief Executive Officer

PURPOSE

To create and implement an ongoing vulnerability scanning process as part of the internal information security risk assessment for the purpose of determining IT security vulnerabilities, and to initiate appropriate remediation.

POLICY

This policy will exist as an adjunct to LAC+USC Policy 461, Information Security Management Process. LAC+USC CIO or designee shall develop and implement a Vulnerability Scanning and Remediation Program as follows:

Vulnerability Scans

LAC+USC CIO shall designate a Vulnerability Scanning and Remediation Program administrator to create, test, and implement an automated, non-intrusive full vulnerability scans using the Countywide / DHS enterprise solution for Vulnerability Scanning and Remediation on the respective networked components. The scans shall comply with the County Network Vulnerability Scanning Standards. The Vulnerability Scanning and Remediation administrator at LAC+USC shall insure that all network segments are included in the scans.

Remediation Plan

The Vulnerability Scanning and Remediation administrator shall implement a remediation process to include an automated patch management solution and other necessary tasks to correct identified vulnerability threats, giving priority to higher impact threats.

High impact vulnerabilities shall be remediated within two weeks of identification.

Medium impact vulnerabilities shall be remediated within one month.

Low impact vulnerabilities shall be remediated within two months.

Identified vulnerabilities that are not remediated or patched within the required time frames will be documented for cause.
LAC+USC workforce members that violate the security policies and procedures will be subject to appropriate corrective actions.

Non-LAC+USC/County workforce members, contractors and agencies that violate the security policies and procedures are subject to sanctions or penalties imposed pursuant to the applicable contract or memorandum of understanding (MOU) and/or federal, state, local law.

DEFINITIONS

Vulnerability

A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.

High Impact Vulnerability

A vulnerability whose exploitation could allow the propagation of an Internet worm without user action. When these vulnerabilities are successfully leveraged, the result is permanent compromise of the attacked systems.

Medium Impact Vulnerability

A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources.

Low Impact

A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

Scan

The use of a tool to search through the components of the network in order to discover answers to questions.

Risk Assessment

The identification and study of the vulnerability of a system and the possible threats to its security.

Remediation process

The agreed process that vulnerabilities, no matter what impact, will be addressed and remediated by the appropriate technical staff. This process will also be reviewed and enforced by IT management and LAC+USC IT Security Compliance Division (SCD).

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I, (460-A) to DHS Policy No. 935.00,
DHS Information Technology and Security Policy.

AUTHORITY

45 Code of Federal Regulations (CFR) Part 164, §164.308(1)(i)
Health Insurance Portability and Accountability Act of 1986 (HIPAA), 42 U.S.C. Sections
  1320-d – 1320-d-8.
Board of Supervisors Policies:
  6.100, “Information Technology and Security”
  6.107, “Information Technology Risk Assessment”

6.108, “Auditing and Compliance”
Countywide Information Security Strategic Plan
County Network Vulnerability Scanning Standards

CROSS REFERENCES

DHS Policies
361.10, “Disciplinary Actions for Failure to Comply with Privacy Policies and Procedures”
747, “Disciplinary Action”
935.00, “DHS Information Technology and Security Policy”
935.01, “Information Security Management Process”

REVISION DATES

September 22, 2017; October 30, 2020