UC Riverside, School of Medicine Policies and Procedures
Policy Title: Vulnerability Management
Policy Number: 950-02-204

Responsible Officer:	Information Security Officer (ISO)
Responsible Office:	UC Riverside School of Medicine (UCR SOM) Compliance Department
Origination Date:	11/02/2016
Date of Revision:	1/19/2017
Scope:	• All UCR SOM information, in an electronic format, regardless of where it resides, who possesses it or who has authority to create, store, transmit or use it. • All Technology Infrastructure owned and/or administered by UCR SOM • All UCR SOM divisions, including those of UCR SOM subsidiaries, if any • All UCR SOM workforce members, including employees, interns, contractors, consultants, and vendors doing business with UCR SOM including any individuals affiliated with third parties that access UCR SOM systems.

I. Policy Summary

The purpose of this policy is to define UCR SOM's enterprise vulnerability management program, including detection, analysis, and remediation. This policy establishes a framework for identifying and promptly remediating vulnerabilities to minimize security breaches associated with unpatched vulnerabilities.

II. Definitions

Please refer to Standard Definitions Guide.

III. Policy Text

Computing devices with access to UCR SOM network resources (i.e. servers, network shares, applications) must be fully scanned regularly, preferably weekly, for vulnerabilities. Any detected vulnerabilities must be remediated in accordance with the specific time frames described in this policy. To ensure that scans are comprehensive and accurate, scans will be performed by users logged in with privileged access on the respective computer device.

Any identified vulnerabilities, either related to missing patches or improper configuration, must be remediated within the timeframes specified below based on the degree of associated severity. For vulnerability remediation, System Administrators should perform appropriate testing and follow existing change management procedures to ensure proper patch installation for affected systems.

A. Approved Scanning Tools

The ISO and Privacy Officer shall be the sole entity to implement an enterprise scanning tool. Use of other vulnerability scanners on the network must have a documented justification for use and requires approval by the ISO and Privacy Officer.

B. Limitation of Scanning

Vulnerability level	Remediation Time Frame	Description
Urgent (5)	ASAP (Not to exceed 30 days)	Intruders can easily gain control of the host, which can lead to the compromise of the entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.
Critical (4)	30 days	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
Serious (3)	30 days	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
Medium (2)	<90 Days	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
Minimal (1)	<90 Days	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

IV. Responsibilities

A. Office of Information Technology (OIT)

- Maintain inventory of IT assets
- Remediate vulnerability as directed within specified timeframes

B. Information Security

- Performing vulnerability scans
- Identifying vulnerability
- Determine appropriate remediation measures
- Submit unresolvable vulnerability to Compliance & Privacy Officer
- Submit quarterly vulnerability report to Compliance Committee

C. Compliance & Privacy Officer

- Approve risk acceptance of exceptions

V. Procedures

Automated vulnerability scanning will be conducted at least monthly. To provide a better opportunity to remediate in a timely fashion vulnerability scans can be conducted bi-weekly.

Information Security department compiles detailed list of vulnerabilities, patches and remediation steps to OIT for remediation. OIT performs remediation steps or provides justification to Information Security for exceptions. Exceptions are reviewed and approved exceptions are submitted to Compliance & Privacy Officer for risk acceptance.

VI. Forms/Instructions (Not Applicable)

VII. Related Information (Not Applicable)

VIII. Revision History (Not Applicable)