UC Riverside, School of Medicine Policies and Procedures
Policy Title: UCR SOM Patch Management
Policy Number: 950-02-222

Responsible Officer:	Information Security Officer (ISO)
Responsible Office:	UC Riverside School of Medicine (UCR SOM) Compliance Department
Origination Date:	12/05/2016
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. • SaaS model infrastructure is specifically not in the scope of this model since those platforms are maintained by the SaaS provider(s)

I. Policy Summary

The purpose of this policy is to define the proper procedures by which UCR SOM patches various types of computing devices, operating systems, and applications within the enterprise. The policy defines measures to ensure effective patch management procedures are in place to mitigate risk of vulnerabilities to those computer systems and applications.

II. Definitions

Please refer to Standard Definitions Guide.

III. Policy Text

UCR SOM requires timely patching in order to maintain the operational availability, confidentiality, and integrity of information technology systems that are managed by UCR SOM.

1. New servers and desktops must be fully patched with the latest approved patches before entering production
2. All systems and applications must be reviewed at least monthly to verify compliance with current software version and patch levels. Where possible, UCR SOM systems and applications must be in line with current vendor supported versions.
3. Owners of systems connected to the UCR SOM network must agree to have their computers scanned for software versions, have the appropriate version installed, and if required, have the computer rebooted by the patch management software.
4. Non-UCR SOM owned devices require up-to-date antivirus definitions, security patches, closed unnecessary ports, as well as approval from the ISO before connecting to any

UCR SOM network.

5. Removing existing patches or blocking installation of any patch without prior written authorization from the Office of Information Technology (OIT) management is a violation of this policy.
6. Any software version change or patch update must be assessed for applicability and potential risk prior to deployment. Software updates and patches must be researched, tested and verified by appropriate personnel before installing on any UCR SOM asset.
7. Any software version change or patch update will be performed within the timescales established from the vulnerability risk assessments. Critical security patches will be deployed to all user workstations at least monthly, and servers must be patched as soon as possible but no longer than 30 days.
8. Any system that stores, processes, or transmits electronic Patient Health Information (ePHI) must be patched every 30 days or when a patch is made available.
9. Departments that directly manage systems outside of OIT control must follow and demonstrate compliance with this policy. This applies to systems hosted outside of the UCR SOM network if these systems store, process, or transmit UCR SOM data.
10. Change Control procedures must be followed, to include advance notification of any system outages and the scheduling of outage windows outside of business hours whenever possible.
11. For any vulnerability that is determined to create an imminent threat to the UCR SOM computing environment, an emergency change control may be used in order to expedite patch deployment.

IV. Responsibilities

OIT will be responsible for coordination of patching efforts. OIT will be responsible for managing the exceptions list and monitoring all remediation efforts towards compliance.

The Compliance department is responsible for vulnerability scanning, identification and risk calculations. The ISO will act as point of contact regarding all security related guidance, advice, and patching efforts including the exception process.

V. Procedures

A. Non-Compliance

Systems that do not comply with this policy will be isolated from the network. The Privacy and Security Sanctions Policy applies to all workforce members who fail to comply with the University of California's Policy and Procedures.

B. Exceptions

All exceptions to this policy require written consent of the ISO and approval, when necessary, from the Compliance Committee. Approved exceptions are interim in nature and must be renewed on an annual basis, or sooner if documented by the exception, with an updated timeline for conformance to this policy. OIT will document and monitor all approved exceptions.

VI. Forms and Attachments (Not Applicable)

VII. Related Information (Not Applicable)

VIII. Revision History (Not Applicable)