**UC Riverside, School of Medicine Policies and Procedures**
**Policy Title:** Anti-Virus and Malware Protection Policy
**Policy Number:** 950-02-209

| | |
|---|---|
| Responsible Officer: | Information Security Officer |
| Responsible Office: | Compliance |
| Origination Date: | (9/5/2017) |
| Date of Revision: | (9/14/2017) |
| Scope: | • All UCR School of Medicine (SOM) information, in its electronic form, regardless of where it resides, who possesses it or who has authority to create, store, transmit or use it;<br>• All Technology Infrastructure owned and/or administered by UCR SOM;<br>• All UCR SOM divisions, including those of UCR Health subsidiaries, if any;<br>• All UCR SOM facilities, including those of UCR SOM subsidiaries, if any; and<br>• 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 requirements regarding the protection of enterprise informational assets from malicious computer virus and malware attacks. It outlines a consistent approach to mitigating issues caused by computer virus and malware to the UCR SOM infrastructure. In addition to this policy, employee training and vigilance is integral to successfully minimizing risk to malicious software. Each workforce member should never open attachments, links or Internet sites from an un-trusted/unknown sender.

## II. Definitions

Please refer to the Standard Definitions Guide.

## III. Policy Text

All computing devices that connect to the UCR SOM IT infrastructure, including all computing devices that connect remotely (e.g., via wireless, VPN, etc.) must be protected with anti-virus/malware software. All anti-virus/malware software must conform to the UCR SOM software standards and must have up-to-date virus definitions. This applies to all server, desktop, and laptop computers regardless of ownership or location.

## IV. Procedures

UCR SOM will maintain and use secure, approved, and effective anti-virus and anti-malware software on a consistent basis. Updates to the virus definitions should be automated and occur at least hourly. In addition, the following controls apply to all anti-virus/malware installations:

A. Anti-virus/malware software must be installed by the Office of Information Technology (OIT), or by the owner of the computer
B. All settings must be password protected and may not be altered in any manner to reduce the effectiveness of the software
C. Each deployment of anti-virus/malware must be configured to ensure, at a minimum, automatic hourly updates of virus definitions
D. OIT will maintain the current standard for anti-virus/malware software and make this available for end users
E. For all quarantined infections, on a system not managed by OIT, a follow-up Helpdesk ticket must be submitted by the system or business owner, to clean and/or reimage suspected systems
F. A computer that is either unprotected by anti-virus software or by other appropriate means, or has become infected may be removed from the network until such time as the situation is remediated, after risk review by OIT and Information Security

## V. Responsibilities

OIT is responsible for:

A. Ensuring the installation of anti-virus/malware software on all UCR SOM owned/managed computing equipment
B. Continually ensuring all UCR SOM owned/managed computing equipment has approved anti-virus/malware software installed, is configured correctly and receiving automated definition updates
C. Responding to infection alerts
D. Documenting response activities to infection alerts
E. Setting configurations on all anti-virus/malware software to require a password and not allowing any unauthorized configuration changes
F. Creating and maintaining a minimum standard for anti-virus/malware

Information Security Officer will be responsible for:

G. Reviewing audit reports of anti-virus/malware infections
H. Reviewing configuration reports of all enterprise anti-virus/malware installations to verify they meet all required settings
I. Reviewing minimum standards for anti-virus/malware software
J. Managing any exceptions to this policy

## VI. References (Not Applicable)

## VII. Revision History

New policy

COMPLIANCE COMMITTEE (10/24/2017)