UC Riverside, School of Medicine Policies and Procedures
Policy Title: Workstation Security Policy
Policy Number: 950-02-225

Responsible Officer:	Information Security Officer
Responsible Office:	Compliance
Origination Date:	1/30/2018
Date of Revision:	N/A
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; • All Technology Infrastructure owned and/or administered by UCR SOM; • All UCR SOM divisions, including those of UCR Health subsidiaries, if any; • All UCR SOM facilities, including those of UCR SOM subsidiaries, if any; and • 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 Health's requirements regarding security for workstations accessing UCR SOM networks, data, or otherwise used for UCR SOM business purposes. This policy will provide guidance for workstations in order to ensure the security of both the information on the workstation, and the information to which the workstation may access.

II. Definitions

Please refer to the Standard Definitions Guide.

III. Policy Text

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity, and availability of sensitive information, including electronic protected health information (ePHI). Access to sensitive information must be restricted to authorized users.

Workforce members using workstations shall consider the sensitivity of the information that may be accessed, and exercise due care to minimize the possibility of unauthorized access of such information.

UCR SOM will implement physical and technical safeguards for all workstations that access its electronic resources, allowing access to authorized users only. All workstations used to access UCR SOM data, especially ePHI, must follow all of the requirements as a UCR SOM owned workstation. This includes workstations purchased by business units and personally owned devices.

IV. Procedures

Appropriate measures to secure workstations include, but are not limited to:

1. Restricting physical access to workstations to authorized personnel only.
2. Securing workstations prior to leaving area to prevent unauthorized access, by implementing screen lockout (no more than 15 minutes), or automatic logout.
3. Physically securing portable workstations, such as laptops, tablets or smart phones, by locking them in a cabinet at the end of the work day or using physical security cables to attach them to furniture.
4. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. (The password must comply with *UCR SOM Policy 950-02-224 - Password Security).*
5. Enabling password requirements that comply with *UCR SOM Policy 950-02-224 - Password Security.*
6. Ensuring workstations are used for authorized business purposes only.
7. Never installing unauthorized software on workstations (OIT will maintain a list of authorized and/or unauthorized software).
8. Never disable or uninstall UCR SOM standard, pre-installed software.
9. Store all sensitive information, including ePHI, only in authorized storage locations.
10. Installing privacy screen filters or using other physical barriers to reduce risk of exposing sensitive data from unauthorized access.
11. Ensuring all workstations use a surge protector (not power strip) or a UPS (Uninterruptable Power Supply or battery backup).
12. Ensuring that all workstations are protected from virus/malware by using an approved anti-virus/malware software, and all definitions are up to date. (This requires enabling real-time protection and scheduled full disk scans).
13. Ensuring that host-based firewalls are enabled and configured to block all inbound traffic that is not explicitly required for the intended use of the device.
14. Ensuring workstations have full disk encryption (FDE), with pre-boot authorization enabled.
15. Ensuring that all workstations are patched according to the *UCR SOM Policy 950-02-222 - Patch Management.*
16. Ensuring that local administrative accounts are only used when required and all routine or daily activities are performed with a non-privileged account.
17. Ensuring that all workstations are recorded in the device inventory, including the function and type of data that is stored, viewed or transmitted on it.

V. Responsibilities

1. OIT (Office of Information Technology) will be responsible for documenting all workstation standards, listing all approved security measures.
2. OIT will be responsible for verifying that all workstations meet the minimum requirements prior to be authorized for business use.
3. The Information Security Officer (ISO) will be responsible for verifying compliance to this policy is being met.
4. The ISO will be responsible for reviewing any exception requests to this policy.
5. The ISO and OIT will work collaboratively to evaluate any tools or software used to meet or enhance the requirements of this policy.

VI. References

UCR SOM Policy 950-02-224 - Password Security
UCR SOM Policy 950-02-222 - Patch Management

VII. Revision History

New policy

Approvals:

Compliance Committee 1-30-2018

Paul Hackman, J.D., L.LM., C.H.C.
Compliance and Privacy Officer,
School of Medicine

Deborah Deas, M.D., M.P.H
Dean, School of Medicine
CEO, Clinical Affairs