I. Policy Summary
This policy establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. All computer accounts must be password protected to help maintain the confidentiality and integrity of electronic data, as well as, to help protect the UCR School of Medicine compute resources and infrastructure. Passwords to UCR School of Medicine accounts and devices must be kept confidential and must not be shared.

II. Definitions
None at the time of publication.

III. Policy Text
One-time-use passwords are initially provided to the users for the first account log-on. Users are required to create a new password known only to them immediately after the initial log-on.

A. UCR School of Medicine NetID
Passwords must:
- Be a minimum of 8 characters in length
- Not be longer than 32 characters
- Have both upper and lower case characters
- Have at least 1 letter(s)
- Have at least 1 digit(s)
- Not be constructed from a dictionary word
- Not be an exact dictionary word match
- Not be your profile ID or name
- Not be your profile ID or name reversed
- Not be your profile ID or name with letters rearranged
- Not be an old password (any of the previous 12 passwords used)
- Not have more than 1 pair(s) of repeating characters
- Contain characters that can be a pattern typed on a Standard (US) keyboard
- Not contain consecutive characters as in "abcd" or arranged on a keyboard “asdfg”

- UCR School of Medicine NetID passwords will expire every 90 days.
- Each user must have a unique, named, individual UCR SOM NetID
- Network and system administrators will be issued a separate, unique named account specifically for elevated access, as outlined in policy “Managing Privileged Access.”

B. Self-Service Portal
UCR SOM NetID Account holders should set up their challenge questions to facilitate self-service password resets (https://password.medsch.ucr.edu/PM/enroll1.asp)
All Information systems must obscure the password during password entry. Displaying asterisks when a user types in a password is an example of obscuring feedback of password information.
UCR SOM NetID Lockout conditions:
- Users failing to logon after 5 times will experience an automatic lockout,
- Lockout duration will be no less than 30 minutes,
- To unlock accounts before 30 minutes the user must call the HELPDESK and provide ID and answer challenge questions

IV. Responsibilities: N/A

VIII. Related Information
- SOM 6.0 Privacy and Security Sanctions Policy
- UCR School of Medicine Policy– Managing Privileged Access
- UCR School of Medicine Policy – Security Awareness and Training
- UCR School of Medicine Policy – Workstation Security
- UCR School of Medicine Policy – Encryption Controls
- Document Retention Policy
- UC Record Retention Schedule

IX. Revision History:
<table>
<thead>
<tr>
<th>Date Revised</th>
<th>Description of Changes</th>
<th>Author</th>
<th>Reviewer</th>
<th>Date Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/15/2016</td>
<td>Initial Draft</td>
<td>Shawn Kelly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3/17/2016</td>
<td>Update</td>
<td>Shawn Kelly</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Approval(s):

Compliance Committee (04/26/2016)