I. Policy Summary
The purpose of this policy is to establish Internet activities that are permissible for use on the UCR SOM’s electronic communication systems. This policy establishes minimum standards for workstation access controls to internet websites based on usage of the workstation within UCR SOM environment. Internet filtering will be implemented to protect and safeguard electronic data from malicious software associated with internet browsing.

UCR SOM-provided computer systems are the property of UCR SOM and are provided to facilitate the effective and efficient conduct of University business. Users are permitted access to the Internet and information resources to assist in the performance of their job functions.

II. Definitions
Please refer to Standard Definitions Guide.

III. Policy Text
A. Acceptable Use
UCR SOM provides access to the Internet and information resources in order to conduct University business. Individuals may use services which are directly related to their position at UCR SOM. Incidental and occasional personal use is permitted provided such use does not:

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.
- This policy addresses security management for all types of sensitive data and systems including research and financial data.
1. Directly or indirectly interfere with UCR SOM operations
2. Involve port scanning or security scanning
3. Execute any form of network monitoring which will intercept data
4. Burden the UCR SOM with noticeable incremental cost
5. Interfere with individuals’ employment or other obligations to the UCR SOM
6. Violate applicable laws, UCOP, or UCR (SOM) policies
7. Disrupt or degrade performance of the UCR SOM network and computing resources
8. Infringe on copyright laws or software license
9. Access data, a server or an account for any purpose other than conducting UCR SOM business, even if an individual has authorized access
10. Represent UCR SOM in the conduct of personal or political activity without prior approval
11. Use peer-to-peer websites
12. Introduce malicious virus activities
13. Download or pirate software
14. Make fraudulent offers of products, items, or services originating from any UCR SOM account
15. Use a UCR SOM computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws
16. Expose UCR SOM to any unnecessary risks

IV. Responsibilities

A. User Responsibilities
   1. Workforce members must not falsify their identity or enable others to falsify their identity.
   2. Workforce members are responsible for all use and activities assigned to their accounts.
   3. Workforce members have a responsibility to promptly report the theft, loss, or unauthorized access of UCR SOM computing equipment to an appropriate authority.
   4. Individuals must not use resources for which they have not been assigned or authorized for use in their job duties.
   5. Workforce members are responsible for exercising good judgement regarding the reasonableness of personal use of UCR SOM resources.

B. Office of Information Technology (OIT) Responsibilities
   1. Implementing and managing Internet filtering technologies

C. ISO and Privacy Officer
   1. Monitoring Internet filtering activities
   2. Updating categories of Internet filtering based on risk
   3. Managing the exception process, as well as the approval, and denial of access requests

V. Procedures

A. Access Restriction Levels
   Workstations throughout UCR SOM will be set to one of the following levels of internet access restriction based on the risk of malicious attack from the internet website visited:
1. Level 1 (Low Risk)
   Highest access restrictions for workstation deployment (primarily for those in public locations). Approved internet site categories for level 1 include children, medical, research, reference, education, and health & medicine.

2. Level 2 (Low – Medium Risk)
   Second highest access restrictions for medical workstations that are shared among staff members but not available to the public. Approved internet site categories for level 2 include categories from level 1, religion, news, insurance, kids sites, government, infrastructure, job search & carrier development, philanthropic & professional, organizations, Google (Academic only), and sexual education.

3. Level 3 (Medium Risk)
   Second lowest access restrictions for administrative (single user, staff workrooms) workstations. Approved internet sites categories for level 2 include categories from level 1 and 2, in addition to arts, games, entertainment, sports, social, beauty, shopping, real estate, streaming media, blogs and forums, social networking, motor vehicle, travel, business computing and internet, finance and investment, alcohol and tobacco, search engines and portals, external email, hobbies and recreation, fashion, society, and culture.

4. Level 4 (High Risk)
   Lowest access restrictions for workstations with open access. Level 4 restrictions allow accessibility to all sites except those categorized as malicious, hacking, phishing and fraud, and adult & inappropriate explicit content. Level 4 access is determined on a case-by-case basis.

B. Prohibited Access
   Partial list of Web Sites which there is prohibited access for levels 1, 2 & 3:
   - Adult and Pornography
   - Dead Sites
   - Shareware and Freeware
   - Peer to Peer
   - Hacking
   - Weapons
   - Pay to Surf
   - Questionable
   - Keyloggers and Monitoring
   - Malware Sites
   - Phishing and Other Frauds
   - Proxy Avoidance and Anonymizers
   - Spyware and Adware
   - Bot Nets
   - SPAM URLs

C. Exceptions
   Level 1-4 exceptions are approved or denied based upon the warranted risk and on the work-related requirements. Users can request an exception for an individual website to be added to the approved list by clicking on the link in the denial message window. The requestor will be required to provide a business need to access the blocked website and the name of their department manager.
D. Monitoring and Blocking
UCR SOM uses a combination of automated technology and manual review to identify systems that are attacking campus information resources, infected with malware, or fail to meet minimum-security requirements. The automated systems use a combination of pre-determined signatures and traffic analysis to collect and store a relevant portion of electronic communications for systems or user accounts identified as a potential threat to the confidentiality, integrity, or availability of UCR SOM network or information. Security staff may manually review these stored collected electronic communications, in accordance with University and UCOP privacy policies as well as the law, to validate the findings or tune the automated systems. The information collected may include source and destination IP addresses, source and destination ports, URLs, and user names.

UCR SOM Security personnel who operate and support electronic communications resources regularly monitor transmissions for ensuring reliability and security of UCR SOM electronic communications resources and services, and in that process might observe certain transactional information or the contents of electronic communications. Except as provided by Policy or law, they are not permitted to seek out transactional information or contents when not germane to system operations and support, or to disclose or otherwise use what they have observed. In the process of such monitoring, any unavoidable examination of electronic communications (including transactional information) shall be limited to the least invasive degree of inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal or confidential information. Except as provided here, systems personnel shall not intentionally search the contents of electronic communications or transactional information for violations of law or policy.

Users or systems that are “red-flagged” and determined to be a threat may be blocked and denied network access until the issue is resolved. Blocked user accounts may be denied access without additional information. UCR SOM will make best efforts to directly contact the account or system owner, but this is not always possible.

The data of separated employees becomes the property of the University and, with Assistant/Associate Vice Chancellor approval, may be accessed to support University operations.

All monitoring activities will adhere to the guidance provided in the UCOP Electronic Communications Policy (http://www.ucop.edu/information-technology-services/policies/electronic-communications.html).

VI. Revision History
New policy