

UC Riverside, School of Medicine Policies and Procedures

Policy Title: Acceptable Use

Policy Number: 950-02-201

Responsible Officer:	Information Security Officer (ISO)
Responsible Office:	Compliance Advisory Services
Origination Date:	(11/21/2016)
Date of Revision:	(10/28/2020)
Scope:	<ul style="list-style-type: none">• All UCR School of Medicine (SOM) Institutional Information, independent of the location (physical or cloud), ownership of any device or account that it used to store, access, process, transmit or control SOM Institutional Information;• All devices, independent of their location or ownership, when connected to a SOM network or cloud service used to store or process SOM Institutional Information;• All SOM Workforce Members, Suppliers, Service Providers and other authorized users of SOM Institutional Information and IT Resources.• This policy addresses security management for all types of data and systems in the SOM, including research and financial activity.

I. Policy Summary

The purpose of this policy is to outline the acceptable access to and use of SOM Institutional Information and IT Resource in accordance with the University of California (U.C.) Policy BFB-IS-3 Electronic Information Security (IS-3). These rules are in place to protect the employee and SOM. Inappropriate use exposes SOM to risks including virus attacks, compromise of network systems and services, and legal issues. This policy establishes minimum standards for IT Resources, acceptable user behavior, and access controls to Internet websites. Internet filtering will be implemented to protect and safeguard IT Resources and Institutional Information from malicious software associated with Internet browsing.

SOM-provided computer systems are the property of 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. Minimum Security

All IT Resources shall have appropriate security controls and configuration in accordance with Minimum Security Standard and Secure Software Configuration Standard as well as in conjunction with IS-3. The SOM ISO may provision additional requirements based on risk or in conjunction with other applicable policy.

B. Acceptable Use

SOM provides IT Resources and access to the Internet and Institutional Information to conduct University business. Individuals may use services which are directly related to their position at SOM. Incidental and occasional personal use is permitted provided such use does not:

1. Directly or indirectly interfere with SOM operations
2. Involve port scanning or security scanning
3. Execute any form of network monitoring which will intercept data
4. Burden SOM with noticeable incremental cost
5. Interfere with individuals' employment or other obligations to the SOM
6. Violate applicable laws, contractual obligations, or UCOP or SOM policies
7. Disrupt or degrade performance of the 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 SOM business, even if an individual has authorized access
10. Represent the U.C. in the conduct of personal or political activity without prior approval
11. Use peer-to-peer websites or software
12. Introduce malicious virus activities
13. Download or pirate software
14. Install or attempt to install unapproved software
15. Make fraudulent offers of products, items, or services originating from any SOM account
16. Use a SOM computing asset to actively engage in procuring or transmitting material that is in violation of sexual violence, sexual harassment or hostile workplace laws
17. Expose the U.C. to any unnecessary risks
18. Utilize anonymization or unauthorized VPN

IV. Responsibilities

A. User Responsibilities

1. Comply with relevant laws, contractual obligations, and IS-3 and supporting standards and SOM policy in accordance with their relevant role and the classification of Institutional Information or IT Resources being handled.
2. Not falsify their identity or enable others to falsify their identity.
3. Are responsible for all use and activities assigned to their accounts.
4. Promptly report the theft, loss, or unauthorized access of Institutional Information or IT Resources to an appropriate authority.
5. Access, use or share SOM Institutional Information only to the extent it is authorized and necessary to fulfill assigned job duties.
6. Exercise good judgement regarding the reasonableness of personal use of SOM resources.
7. Not circumvent authentication or security of any IT Resource; must support efforts to safeguard IT Resources and Institutional Information.
8. Be subject to security and network monitoring, which may be un-obfuscated, by authorized individuals in conjunction with other applicable policy.
9. Promptly comply with requests from other departments to facilitate this and other applicable policy.

B. Office of Information Technology (OIT) Responsibilities

1. Ensure through legal or technical means that Institutional Information and IT Resources are protected in accordance with Minimum Security Standard and Secure Software Configuration Standard as well as in conjunction with IS-3.
2. Monitor access to Institutional Information and IT Resources for compliance with legal requirements, contractual obligation, applicable policy, and security incident.
3. Implement and manage Internet filtering technologies.

C. ISO and Privacy Officer Responsibilities

1. Audit for compliance with IS-3 and other applicable policy through various methods.
2. Monitor Internet filtering activities and update filtering categories based on risk.
3. Monitor access to Institutional Information and IT Resources for compliance with legal requirements, contractual obligation, applicable policy, and security incident.
4. Manage the Security Exception process, as well as the approval and denial of access requests.

V. Procedures

A. Access Restriction Levels

Workstations throughout SOM will be set to one of the following Protection Levels (PL) based on what Institutional Information is accessed, in accordance with IS-3 and Data Classification Standard:

- PL4 (High Risk)
Highest access restrictions for workstation deployment. Approved Internet site categories for PL4 include children, medical, research, reference, education, and health & medicine.
- PL3 (Medium – High Risk)
Second highest access restrictions. Approved Internet site categories for PL3 include categories from PL4, religion, news, insurance, kids sites, government, infrastructure, job search & carrier development, philanthropic & professional, organizations, Google (Academic only), and sexual education.
- PL2 (Medium Risk)
Second lowest access restrictions. Approved Internet sites categories for PL2 include categories from PL 3 and 4, 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.
- PL1 (Low Risk)
Lowest access restrictions with open access and availability to the public. PL1 restrictions allow accessibility to all sites except those categorized as malicious, hacking, phishing and fraud, and adult & inappropriate explicit content. These systems should be segmented separately and not used for regular business or to access internal resources; PL1 access is determined on a case-by-case basis.

B. Prohibited Access

Partial list of Web Sites which there is prohibited access for PLs 2, 3 & 4:

- 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
- Uncategorized
- Identified malicious sites

C. Exceptions

PL 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

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 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 and contractual obligation, to validate the findings or tune the automated systems.

SOM Security personnel who operate and support electronic communications resources regularly monitor transmissions for ensuring the reliability and security of 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, contract requirement, 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. 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.

VI. References

SOM must adhere to systemwide and relevant UCR policy

- <https://medschoolcompliance.ucr.edu/policies-procedures>

- <https://security.ucop.edu/policies/>
- <https://www.ucop.edu/information-technology-services/policies/index.html>
- <https://security.ucop.edu/policies/it-policy-glossary.html>
- <https://www.ucop.edu/ethics-compliance-audit-services/compliance/hipaa/>
- https://sbs.ucr.edu/campus-merchant-resources#pci_policies
- <https://registrar.ucr.edu/resources/ferpa/UCR-policy>
- <https://its.ucr.edu/cybersecurity/policies-standards>

VII. Revision History

Date Revised	Description of Changes	Author
11/21/2016	New Policy	Shawn Kelly
10/12/2020	Update	Matthew Summerville


Approvals:

COMPLIANCE COMMITTEE (01/27/2021)

 PAUL HACKMAN, J.D., L.L.M.
 CHIEF COMPLIANCE AND PRIVACY OFFICER,
 SCHOOL OF MEDICINE

04/22/21

 DATE



 DEBORAH DEAS, M.D., M.P.H.
 VICE CHANCELLOR, HEALTH SCIENCES
 DEAN, SCHOOL OF MEDICINE

04/22/21

 DATE