

Request for Comments on Policy, Standard, or Guideline Being Proposed for Adoption by IT Governance

Title: UCSF Authorized and Acceptable Use Policy

Date: December 12, 2006

Version: 1.0

Status: Initial Submission

Comment Period:

Text of Policy, Standard, or Guideline being Proposed:

The Authorized and Acceptable Use Policy formally defines the scope of Authorized and Acceptable use of UCSF Electronic Information Resources.

Summary of Proposal:

Use of UCSF Electronic Information Resources is governed by federal, state and University policy. This document formally defines UCSF's Authorized and Acceptable Use and is consistent with other UC Campuses. The University requests that Campuses develop Authorized and Acceptable use policies in order to ensure Campus compliance with existing policies and law.

Target Audience for Proposal

This policy applies to all UCSF faculty, staff, students and users of UCSF Electronic Resources.

Committee or Subcommittee Submitting Proposal:

Information Security Committee

Contact within Committee or Subcommittee:

Stephen Lau Stephen.Lau@ucsf.edu (415) 476-3106	Carl Tianen Carl.Tianen@ucsf.edu (415) 502-1593
---	---

Details of Policy, Standard, and/or Guideline Being Proposed

1. Introduction

The University of California (University) recognizes and encourages the use of Electronic Information Resources (*Resources*) in support of the University's mission of education, research, community service, patient care and to conduct University business. This Authorized and Acceptable Use Policy formally defines the scope of Authorized and Acceptable use of UCSF *Resources*.

2. Scope

This Policy applies to all users of UCSF *Resources* and to all *Resources* that are used for UCSF related business or are connected to University owned networks. This includes personal and other devices, such as third party systems, that are not owned by the University, but are used primarily for UCSF business purposes or are connected to University owned networks. All Authorized Users (Users) are responsible for reading, understanding and complying with this Policy. Refer to Section 8 for a further description of *Resources* and *Authorized Users*.

Situations or conditions related to Authorized and Acceptable Use not covered by this Policy may be covered by federal, state or local law and other University policies; see *Associated Policies and Procedures* and *References*.

3. Privacy

The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and conversations and has established policies and procedures consistent with federal and California law to guide the conduct of University activities relating to the use of *Resources*. This Policy reflects these principals within the context of the University's legal and other obligations.

UCSF does not routinely inspect, monitor or disclose electronic communications, except under certain circumstances. UCSF may deny or restrict access and usage of *Resources* for violations of this Policy. Further information can be found in the UC Electronic Communications Policy (ECP), the UCSF Network Security Monitoring Policy and in the Implementation section of this Policy.

4. Associated Policies and Procedures

- University of California Electronic Communications Policy (ECP)
- University of California Business and Finance Bulletin, IS-3, Electronic Information Security
- University of California Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities
- UCSF 650-16 Information Security and Confidentiality
- UCSF Network Security Monitoring policy

5. Definitions

The following terms are defined in Section 8 of this Policy.

- Authorized Individual/User (User)

- Computer Support Coordinator (CSC)
- Electronic Information Resource (Resource)
- Exceptions to Policy
- Resource Proprietor
- Restricted Information

6. Policy

This Policy does not prohibit units within UCSF from having additional Authorized and Acceptable Use policies and guidelines due to legal constraints or business requirements. Deviations from this Policy, however, must be documented and be made available to affected Authorized Individuals.

A. Authorized Use

Usage of and access to UCSF *Resources* is limited to *Authorized Users* and is considered a privilege, not a right. UCSF reserves the right to revoke or curtail access privileges at any time. UCSF does not provide any guarantee for availability and reliability of *Resources*.

Access by *Authorized Users* shall be limited to the minimum needed to further the University's mission and to conduct University business. Controls should be utilized to minimize risk of abuse and/or information security incidents.

For the purposes of this Policy, users of *Resources* meant for public use, including but not limited to Internet kiosks and publicly accessible web servers are considered Authorized Users and fall within the scope of this policy.

B. Acceptable Use

Acceptable Use of *Resources* includes any use to conduct University business, to further the University's mission and *Incidental Personal Use* as defined below. Unacceptable Use includes, but is not limited to, violations of the following actions.

- 1) **Copyrights and Licenses** - Users shall respect all copyrights and licensing agreements.
 - a. Copying
 - i. Software shall not be copied except as permitted by copyright law or a license agreement.
 - b. Number of simultaneous users
 - i. The number and distribution of copies shall be handled in such a way that the number of simultaneous users does not exceed the number of copies purchased, unless otherwise stipulated in the purchase contract.
 - c. Plagiarism
 - i. Copied material shall be properly attributed. Plagiarism of electronic information is subject to the same sanctions as in any other medium.
- 2) **Integrity** - Users shall not interfere with the normal operation of any *Resources*.

- a. Modification, damage, or removal
 - i. Users shall not intentionally modify, damage, or remove *Resources* that are owned by the University or Users without proper authorization from UCSF or the owner of the *Resource*.
 - b. Encroaching on others' access and use
 - i. Users shall not intentionally encroach on others' access and use of *Resources*. This includes but is not limited to: the sending of chain-letters or excessive messages (size or volume); printing excessive copies; running grossly inefficient programs when efficient alternatives are available; unauthorized modification of *Resources*; attempting to disable or prevent authorized access to *Resources*.
 - c. Unauthorized or destructive programs
 - i. Users shall not intentionally develop or use programs such as, but not limited to, viruses, backdoors, and worms that disrupt other Users, access private or restricted portions of the system, identify security vulnerabilities, decrypt secure data, or damage the software or hardware components of a *Resource*. Legitimate academic pursuits for research and instruction that are conducted under the supervision of academic personnel are authorized to the extent that the pursuits do not compromise the University's *Resources*.
 - d. Disabling, modifying, testing or circumventing security controls
 - i. Users shall not intentionally disable, modify, test or circumvent any *Resource* security controls without authorization. This includes but is not limited to: disabling or circumventing authorization and authentication mechanisms; intentionally disabling, modifying or removing security logs; intentionally causing a security control to fail; running any programs that intentionally create numerous security control false positives; modifying networks to circumvent security monitoring or access controls; intentionally causing or creating the perception of an information security incident.
- 3) **Unauthorized Equipment** - Users shall not install or attach any equipment to a UCSF *Resource* without the approval of the owner, system administrator or CSC for that *Resource*.
- a. Examples of equipment include: wireless access points, modems, disk drives, networking devices, personally owned computers and flash memory.
- 4) **Access** - Users shall not seek or enable unauthorized access.
- a. Authorization
 - i. Users shall not access *Resources* without proper authorization, or intentionally enable others to do so.
 - b. Authorization levels
 - i. User access levels shall not be greater than that required to conduct University business; i.e. a User who does not conduct system administration on a *Resource* should not be given system administrator privileges on that *Resource*.

- ii. Users shall not attempt to obtain a higher authorization level without need and permission.
 - c. Password protection
 - i. A User who has been authorized to use a password-protected account shall not disclose the password or otherwise make the account available to others.
 - ii. Sharing of accounts is prohibited. Other methods, such as shared file permissions or temporary passwords should be used if data needs to be shared.
- 5) **Use of Electronic Communication Records** - Users may seek out, use, or disclose electronic communication records only for UCSF business in compliance with the UCSF Network Security Monitoring Policy and the ECP.
- 6) **Usage** - Users shall comply with all applicable law and University policy.
 - a. Hostile working environment
 - i. Users shall not use *Resources* in a manner that creates a hostile working environment (including sexual or other forms of harassment), or that violates obscenity laws.
 - b. Unlawful activities
 - i. Users shall not use *Resources* for unlawful activities or activities that violate University policy, including fraudulent, libelous, slanderous, harassing, threatening, or other communications.
 - c. Mass messaging
 - i. Users shall avoid spamming, and other inappropriate mass messaging to newsgroups, bulletin boards, mailing lists, or individuals. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list so long as the material is consistent with the list's purpose.
 - d. Information belonging to other Users.
 - i. Users shall not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other Users without the permission of those other Users.
 - e. False identity
 - i. Users shall not use the identity of another User without the explicit approval of that User, or mask the identity of an account or machine.
- 7) **Implying University Endorsement** - Users shall not imply University endorsement of products or services of a non-University entity from a *Resource* without approval. Users shall not give the impression that the User is representing, giving opinions, or otherwise making statements on behalf of the University unless authorized to do so. To avoid this, the User may use a disclaimer such as "The opinions or statements expressed herein should not be taken as a position of or endorsement by the University of California."
- 8) **Protection of Restricted Information** - Users are responsible for maintaining the security of restricted information. Refer to Section 8 for a definition of Restricted Information. Restricted Information that is not necessary for a User to conduct

University business shall be removed from the *Resource* or shall have authorizations set such that it is inaccessible from that User.

- 9) **Political or Religious Use** – UCSF is a not-for-profit, tax-exempt organization and, as such, is subject to federal, state, and local laws on the use of University property.
 - a. Political or religious use.
 - i. In communications relating to religious or political activities or issues, the User's UCSF title may be used only for identification. If such identification might reasonably be construed as implying the support, endorsement, or opposition of UCSF with regard to any religious or political activity or issue, a disclaimer shall be used, e.g. "The opinions or statements expressed herein should not be taken as a position of or endorsement by the University of California."
- 10) **Incidental Personal Use** – Authorized Users may use *Resources* for Incidental Personal Use purposes provided that such use does not: (a) directly or indirectly interfere with the University's operation of electronic communications resources; (b) interfere with the user's employment or other obligations to UCSF; (c) burden UCSF with noticeable incremental costs; (d) violate the law or UCSF policy.
 - a. Users are responsible for ensuring any Incidental Personal Use falls within this scope and may be held liable for any damages to UCSF associated with Incidental Personal Use.
 - b. Any Incidental Personal Use may become University records and subject to disclosure to the University and third parties.
 - c. Examples of Incidental Personal Use include, but are not limited to: visiting non work related websites; sending personal emails; using instant messaging services for personal communications; accessing media for which the User has access rights.
- 11) **Commercial Use** - *Resources* shall not be used for non-University commercial purposes, except as permitted under University policy or with the appropriate approval.
- 12) **Advertisements** - *Resources* shall not be used to transmit commercial or personal advertisements, solicitations, or promotions, except as permitted under University policy and with the appropriate approval.
- 13) **Non-University Sites and Resources** - External non-University sites and resources that are accessible through UCSF *Resources* may have their own policies governing their use. Users are responsible for understanding and following UCSF policies and/or the remote resources' policies, whichever are more restrictive.

C. Administrative and Authorization Management

Resources shall utilize physical and logical authentication and authorization controls in accordance with University policy and appropriate to the risk level for that Resource.

Unauthenticated access and/or authorization shall only be granted if specifically needed for an operational requirement or in instances where authentication and/or authorization are not technically feasible. Examples include but are not limited to, public Internet kiosks, web servers meant for public access, access to information meant for public access. Additional security controls, such as monitoring and logging shall be deployed in such instances to reduce the risk of abuse and/or information security incidents. Refer to IS-3 for more information about appropriate controls.

Access to Restricted Information *must* utilize authentication and authorization. Restricted Information must not reside on a Resource that allows unauthenticated access and/or authorization.

1) Account Management

- a. Accounts may only be granted to Authorized Users and must be associated to an identifiable person. An example of an identifiable person is someone who is granted a UCSF ID number.
- b. Accounts granted to a User who is not a UCSF faculty, staff or student must designate a UCSF faculty or staff member as being responsible for the account. Refer to the UCSF Guest Access form. Guest Access must be reviewed and approved by an appropriate UCSF authority, such as a Department chair or a Dean, to ensure appropriateness of request.
- c. Units responsible for granting access are responsible for ensuring timely removal of accounts and for ensuring proper access levels are maintained.
- d. Units are responsible for reviewing their accounts on a regular basis, at least once a calendar year, to ensure that all users are still Authorized Users and have appropriate access levels, and to remove or modify access where appropriate.
- e. Persons who lose their affiliation with UCSF, i.e. they are no longer Authorized Users, shall have their accounts and access removed within a reasonable time frame, not exceeding 180 days. Refer to Section 8 for a definition of “Authorized User” and affiliation.
 - i. For example: an employee leaves UCSF employment. Their UCSF accounts should be disabled as soon as possible upon termination, not to exceed 180 days past their separation date.
- f. Accounts with access to Restricted Information *must* be terminated or have their access modified to prevent access to Restricted Information immediately upon a User’s loss of affiliation with UCSF. Any variations must be documented as an *Exception to Policy*.
- g. Records of access approvals to Restricted Information should be retained consistent with University Records Disposition Program and Procedures (BFB RMP-2).

- h. Accounts for employees who lose their affiliation by termination must be disabled or removed on the same day of termination.
- i. An account that is not deleted upon loss of affiliation shall be transferred to another UCSF faculty or staff person designated as being responsible for the account.
- j. An individual who terminates their UCSF affiliation, but still requires access to UCSF *Resources*, shall have their access privileges modified to restrict access to only that required. All such Users shall be associated with a UCSF faculty or staff member who is capable of ensuring their continued access requirements and must have their access and affiliated UCSF faculty or staff member documented. Access by such individuals must be reviewed no less than once per year to ensure access is still required. Refer to the UCSF Guest Access form.
 - i. For example: a researcher leaves UCSF, however there is an operational need to occasionally collaborate with UCSF colleagues. Access may be granted, however a UCSF faculty or staff person must be appointed as being responsible for this individual, the access should be restricted to the minimum needed, reviewed on a periodic basis and terminated when it is no longer needed.
- k. Accounts without activity for over 6 months (dormant accounts) should be disabled and reviewed for possible deletion.

7. Implementation

Implementation of this Policy is the responsibility of all Departments and Schools within UCSF and all Users. All Users are responsible for understanding this Policy and ensuring their use falls within the scope of this Policy.

Deviations from this Policy must be documented and made available to affected Users. Temporary or minor deviations to this Policy may be handled as *Exceptions to Policy* and must be documented.

8. Violations

Minor or accidental violations of this Policy may be handled informally, either through electronic email, education or discussion.

More serious or repeated violations of this Policy may result in temporary or permanent loss of access privileges or modification of these privileges.

Violators may be subject to disciplinary action up to and including dismissal or expulsion under applicable University policies and collective bargaining agreements. Violators may also be subject to any federal or state penalties for violations.

Individuals who become aware of a violation or of a potential violation of this Policy should inform their supervisor, department head, or Internal Audit.

In the event of a violation of this Policy that involves possible unlawful action by an individual, the Locally Designated Official, the employee's immediate supervisor, or other appropriate official should immediately be notified in accordance with the [Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities](#) (the "Whistleblower Policy"). Notification should take place before any action is taken, unless prompt emergency action is required to prevent bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policy, or significant liability to the University or to members of the University community.

Resources found in violation of this Policy may be removed from the UCSF network or prohibited from connecting to the UCSF network until the violation is mitigated. Notifications of disconnects will be communicated to the Resource Proprietor as quickly as possible, however Resources may be disconnected prior to notification.

UCSF may disconnect or limit access to a *Resource*, groups of *Resources*, the UCSF network and the Internet without notice in order to protect *Resources*, both external and internal, under exigent circumstances.

9. Definitions

Authorized Individual/User (User)

A University employee, student, or other individual affiliated with the University who has been granted authorization by the Resource Proprietor, or his or her designee, to access a Resource and who invokes or accesses a Resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with the University. The authorization granted is for a specific level of access to the Resource as designated by the Resource Proprietor, unless otherwise defined by University policy. Examples of Authorized Users include but are not limited to the following:

- UCSF faculty, staff and students
- The general public for publicly accessible *Resources*.
- Individuals who are collaborating with UCSF researchers and are granted access to UCSF data or resources.
- Business partners with legitimate business need to access UCSF resources.

Computer Support Coordinator (CSC)

UCSF staff member that provides comprehensive support for computing technology within a defined department.

Electronic Information Resource (Resource)

A resource used in support of University activities that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, data – in raw, summary, and interpreted form – and associated computer server, desktop (workstation), portable devices (laptops, PDAs) or media (CD ROM, memory sticks, flash drives) communications and other hardware used to conduct activities in support of the University's mission.

Exceptions to Policy

Any *Resources* or activities in violation of Policy, but are allowed due to business need or operational requirement. All Exceptions to Policy must be documented and reviewed by Enterprise Information Security to assess the appropriateness and impact of the exception. Documentation must include requestor, policy exception, reason for exception and length of time. Documentation can be of the form of email, paper document or an electronic document.

Resource Proprietor

The individual designated responsible for the information and the processes supporting the University function. Resource Proprietors are responsible for ensuring compliance with federal or state statutory regulation or University policy regarding the release of information according to procedures established by the University, the Campus, or the department, as applicable to the situation. Responsibilities of Resource Proprietors may include, for example: specifying the uses for a departmentally-owned server; establishing the functional requirements during development of a new application or maintenance to an existing application; and determining which individuals may have access to an application or to data accessible via an application. All Electronic Information Resources are University resources, and Resource Proprietors are responsible for ensuring that these Resources are used in ways consistent with the mission of the University as a whole.

Restricted Information

The term *restricted information* describes any confidential or personal information which is protected by law or policy and that requires the highest level of security protection, whether in storage or in transit. See BFB IS-2 for further discussion on Restricted Information.

Examples of Restricted Information include:

- Personally Identifiable Information protected by SB1386
 - e.g. SSN number , driver license information, financial account information
- Electronic Protected Health Information (ePHI)
- University financial information
- Proprietary information
- Information that, if disclosed, would cause embarrassment or damage to the University.

10. References

- Electronic Communications Policy - <http://www.ucop.edu/ucophome/policies/ec/>
- UCSF Policy 650-16 Information Security and Confidentiality - <http://policies.ucsf.edu/650/65016.htm>
- UC Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (Whistleblower Policy) - <http://www.ucop.edu/ucophome/coordrev/policy/10-04-02whistle.pdf>
- Definition of a CSC - http://its.ucsf.edu/information/support/csc_roles.jsp

Benefits to UCSF and Individuals

Existing UCSF policies do not adequately address Authorized and Acceptable use. Some departments and schools have developed their own interpretations of Authorized and

Acceptable use, which may or may not be in violation of existing laws or policies, while others have not. The University encourages Campuses to develop Campus-wide Authorized and Acceptable Use policies to encourage consistent application of existing law and policies.

Known Limitations

None

Impact

- **Technical Impact**

None

- **Budgetary Impact**

	One-Time	Ongoing
Central	None	None
Departmental	None	None
End user	None	None

- **Operational/Functional Impact**

None

Compliance Issues

All members of UCSF are responsible for complying with this policy. Refer to Section 8 of the RFC for violation implications of this policy.

Security Issues

No new security issues are introduced.

Acknowledgments

This RFC was developed by Enterprise Information Security in conjunction with the Information Security Committee.

Glossary

- Authorized Individual/User (User)
- Computer Support Coordinator (CSC)
- Electronic Information Resource (Resource)
- Exceptions to Policy
- Resource Proprietor

- Restricted Information

Related standards

The following are examples of similar Acceptable and Authorized Use policies at

- UC Davis Acceptable Use Policy - <http://manuals.ucdavis.edu/ppm/310/310-23a.pdf>
- UC San Diego Acceptable Use Policies - <http://www-ac.s.ucsd.edu/lib/aup.php>
- UC Berkeley Guidelines for Administering Appropriate Use of Campus Computing and Network Services - <http://itpolicy.berkeley.edu/approp.use.html>

External documents, UC Policies and or standard-setting organizations referenced

- Electronic Communications Policy - <http://www.ucop.edu/ucophome/policies/ec/>
- UCSF Policy 650-16 Information Security and Confidentiality - <http://policies.ucsf.edu/650/65016.htm>
- UC Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (Whistleblower Policy) - <http://www.ucop.edu/ucophome/coordrev/policy/10-04-02whistle.pdf>
- Definition of a CSC - http://its.ucsf.edu/information/support/csc_roles.jsp

Suggested product(s)

Not applicable.

Responsibility for Implementation

All members of UCSF are responsible for implementation of this policy.

High-Level Implementation Strategy and Approximate Timeline

Policy will become effective as soon as approved.

Person(s) or Group(s) With Ongoing Operational Responsibility for the Policy, Standard, or Guideline.

Enterprise Information Security and the UCSF Information Security Committee

Key Issues Raised by Comments Received To Date and How Addressed or Resolved