

Office of Research Acceptable Computer Use Policy - Summary

Proprietary Information

1. Keep passwords secure and do not share accounts.
2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation set at 15 min. or less, or by logging-off when the host will be unattended.
3. Postings by employees from a UCSF email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of UCSF, unless posting is in the course of business duties.
4. All hosts used by the employee that are connected to the UCSF Internet/Intranet/Extranet, whether owned by the employee or UCSF, shall be continually executing approved virus-scanning software.
5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

Strictly prohibited activities, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UCSF.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of copyrighted software for which UCSF/OR or the end user does not have an active license.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses).
5. Revealing your account password to others or allowing use of your account by others.
6. Using a UCSF/OR computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
8. Port scanning or security scanning is **expressly prohibited** unless prior notification to OR-IT is made.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language or size of messages.
3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
5. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Please refer to the Office of Research web site for the detailed policy statement.