



Computer Lab Use and Security Policy

Policy Contents	Effective Date: 03-01-2015
I. POLICY STATEMENT	Last Updated: 02-20-2015
II. REASON FOR POLICY	Responsible University Officer:
III. SCOPE	Opinder Bawa Vice President, Chief Information Officer
IV. AUDIENCE	Policy Owner:
V. POLICY TEXT	Director, Client Support Services
VI. PROCEDURES	Policy Contact:
VII. RELATED INFORMATION	ITS Help Desk
VIII. DEFINITIONS	
IX. FREQUENTLY ASKED QUESTIONS	
X. REVISION HISTORY	
XI. COMPLIANCE	
XII. POLICY EXCEPTION PROCESS	
XIII. APPENDICIES	



I. POLICY STATEMENT

A. The ITS computer labs are designated for use by current students, faculty, and staff of the University of San Francisco. By using any computer in the ITS computer labs at USF, you agree to abide by this policy.

II. REASON FOR POLICY

A. This policy is intended to ensure the ITS general-purpose computer labs provide computer equipment in a secure, respectful environment to help USF students, faculty and staff be productive.

III. SCOPE

A. This policy covers the use of the ITS computer labs at USF.

IV. AUDIENCE

A. This policy is intended for all USF students, faculty and staff who use the ITS computer labs.

V. POLICY TEXT

A. No food or drinks allowed in the computer labs at any time.

B. No shouting, loud talking or cell phone use allowed inside the labs.

C. Students are not permitted to install, modify or delete any software on lab computers.

D. If a station is left unattended for more than 20 minutes, another person may use the machine.

E. Scheduled classes in the labs have priority over all other uses.

F. Do not save files or other work on lab machines. The hard drive is wiped clean every time the computer is restarted. User data files should be saved on flash drives or Google Drive.

G. ITS is not responsible for problems caused by computer viruses, improper use of the equipment, or loss of data due to equipment malfunctions or any other reason.

H. Equipment in the computer labs may not to be removed, modified, relocated, or disassembled without permission of the Lab Coordinator.

I. Do not post signs in the lab or on the lab doors without first seeking the permission of the Lab Specialist.

J. ITS computing resources may not be used for illegal or disruptive purposes.



- K. Reproduction of any copyrighted material (e.g. software, music, video, books, photographs, etc.) is prohibited.
- L. Displaying of offensive graphic images in ITS labs is not permitted.
- M. Sending/posting harassing or unwanted messages to others is prohibited.
- N. Intentionally seeking information on, obtaining copies of, or modifying files, tapes, or passwords belonging to other users, or misrepresenting others, unless explicitly authorized to do so by those user, is prohibited.
- O. Be respectful of other lab users, lab equipment and area at all time in the computer labs.
- P. Problems with computer lab equipment should be reported to the lab personnel immediately.
- Q. Users are to clean up the area around the computer they used before they leave.
- R. Network ports in computer labs are for lab equipment only. No other devices may be connected to them.
- S. **Protect your security.** Log off the computer before leaving the computer lab.

VI. PROCEDURES

- A. To Use the Virtual Computer Lab
 1. You can gain access to the full USF Windows Lab software suite through your own personal computer anywhere so long as you have: (1) a current Windows or Apple computer, (2) a high-speed internet connection, and (3) a valid USFconnect account.
 2. To use the Virtual Computer Lab, log in using your USFconnect username and password at <https://virtuallab.usfca.edu> on a supported web browser on your laptop or desktop. If this is your first time logging on, you will be asked to install the Citrix XenApp client.
 3. Click on the USF Virtual Lab icon. If a security pop-up displays, click “Allow”. The system will first set up your session and then you will see the Windows 7 virtual desktop.
 4. **Note:** Files are not saved when you log out of the Virtual Computer Lab.

VII. RELATED INFORMATION

- A. (None)

VIII. DEFINITIONS

- A. (None)



IX. FREQUENTLY ASKED QUESTIONS

- A. (None)

X. REVISION HISTORY

- A. 04-16-2007 – First publication
- B. 02-20-2015 – Updated to the new format

XI. COMPLIANCE

- A. Failure to follow this policy can result in disciplinary action in accordance with [Human Resources](#) Employment Handbook and [Office of General Counsel](#) employee and labor relations. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

XII. POLICY EXCEPTION PROCESS

- A. A proposed exception request to ITS Policy requires a formal e-mail explanation related and in support of job function.
- B. A proposed exception request to ITS Policy, mentioned in 'XII.A', must be approved via email by respective department or division supervisor, Dean, or VP, before submitted to ITS for review.
- C. Forward approved email as stated in 'XII.B' to itshelp@usfca.edu for processing.
- D. Evaluation of ITS Policy Exception will escalate internally, and as applicable may include further review by: UITC subcommittee(s), the Information Security Officer, and others as appropriate at the request of VP for IT.

XIII. APPENDICIES

- A. (None)