

Remote Access Policy

Participation in a remote access program may not be possible for every employee. Remote access is meant to be an alternative method of meeting Office of Research needs. The Office of Research may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

1.0 Purpose

The purpose of this policy is to define standards for connecting to UCSF Office of Research's network from any host. These standards are designed to minimize the potential exposure to UCSF Office of Research from damages, which may result from unauthorized use of UCSF Office of Research resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical UCSF Office of Research internal systems, etc.

2.0 Scope

This policy applies to all UCSF Office of Research employees, contractors, vendors and agents with a UCSF Office of Research-owned or personally-owned computer or workstation used to connect to the UCSF Office of Research network. This policy applies to remote access connections used to do work on behalf of UCSF Office of Research, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of UCSF Office of Research employees, contractors, vendors and agents with remote access privileges to UCSF Office of Research's UCSF network to ensure that their remote access connection is given the same consideration as the user's on-site connection to UCSF Office of Research.
2. General access to the Internet for recreational use by immediate household members through the UCSF Office of Research Network on personal computers is permitted for employees that have flat-rate services. The UCSF Office of Research employee is responsible to ensure the family member does not violate any UCSF Office of Research policies, does not perform illegal activities, and does not use the access for outside business interests. The UCSF Office of Research employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the UCSF network via remote access methods, and acceptable use of UCSF Office of Research's network:
 - a. *Acceptable Encryption Policy*
 - b. *Virtual Private Network (VPN) Policy*
 - c. *Wireless Communications Policy*
 - d. *Acceptable Use Policy*

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

2. At no time should any UCSF Office of Research employee provide his or her login or email password to anyone, not even family members.
3. UCSF Office of Research employees and contractors with remote access privileges must ensure that their UCSF Office of Research-owned or personal computer or workstation, which is remotely connected to UCSF Office of Research's UCSF network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. UCSF Office of Research employees and contractors with remote access privileges to UCSF Office of Research's network must not use non-UCSF Office of Research email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct UCSF Office of Research business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the UCSF Office of Research network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and IT group must approve security configurations for access to hardware.
9. All hosts that are connected to UCSF Office of Research internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to UCSF Office of Research's networks must meet the requirements of UCSF Office of Research-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the UCSF Office of Research production network must obtain prior approval from IT group.