

Remote Access Policy - Summary

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. 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.

Here is a list of "Password don'ts":

- Don't reveal a password over the phone to ANYONE
 - Don't reveal a password in an email message
 - Don't reveal a password to the boss
 - Don't talk about a password in front of others
 - Don't hint at the format of a password (e.g., "my family name")
 - Don't reveal a password on questionnaires or security forms
 - Don't share a password with family members
 - Don't reveal a password to co-workers while on vacation
3. 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.
 4. Non-standard hardware configurations must be approved by Remote Access Services and IT group must approve security configurations for access to hardware.
 5. 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, including personal computers.
 6. 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.
 7. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to UCSF Office of Research internal networks.
 8. VPN users will be automatically disconnected from UCSF Office of Research's network after TWENTY (20) minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
 9. Only UCSF approved VPN clients may be used.
 10. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of UCSF Office of Research's network, and as such are subject to the same rules and regulations that apply to UCSF Office of Research-owned equipment, i.e., their machines must be configured to comply with UCSF's Security Policies.