



UCSF Minimum Security Standards Checklist for Electronic Resources

All campus systems must comply with UCSF Minimum Security Standards. For questions or assistance, or if you answer **NO** to any of the questions below, please contact Customer Support at 514-4100 (option 1 for Medical Center IT, option 2 for OAAIS), or online at <http://help.ucsf.edu/>. Other resources can be found at <http://security.ucsf.edu/>.

Name:	Department:	Response
Date:	System:	

Passwords

Are your passwords at least 7 characters long and a mix of alphanumeric characters per the UCSF Password Standards (<http://oaais.ucsf.edu/OAAIS/1174-DSY.html>)?

Do you change your password at least every 180 days?

Physical Security

Is your system set to auto-lock and does it require a password for access after a twenty-minute (or less) period of inactivity?

Anti-virus Software

Is anti-virus software installed and enabled on your computer?

Firewall Software

Is firewall software installed and enabled on your computer?

Email and Encryption of Confidential Information

Do you know how to encrypt email to protect confidential information?

Do you encrypt any email containing protected health information or other confidential information?

When connected remotely, is your connection via the campus Virtual Private Network (VPN)?

If you have patient health information or other confidential information on a portable device (i.e., a laptop, BlackBerry, etc.), is it encrypted?

Software Updates and Patches

Are all of your systems patched or updated in a timely fashion?

Unnecessary Services

Have you disabled or removed all unnecessary services on your systems?

Comments: