



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

Do all systems enforce password guidelines compliant with UCSF standards (see <http://oaais.ucsf.edu/OAAIS/1174-DSY.html>)?

Are users required to change pre-assigned passwords immediately?

Have you modified all default passwords for network-accessible devices and systems?

Physical Security

Are all devices and systems set to auto-lock and do they require a password for access after a twenty-minute (or less) period of inactivity?

Anti-virus Software

Is anti-virus software installed, *enabled*, and current on all systems?

Firewall Software

Is firewall software installed and *enabled* on all laptops, desktop machines, and servers?

Email and Encryption of Confidential Information

Do all users in your department know how to encrypt email to protect confidential information?

Is all email containing protected health information or other confidential information encrypted?

Is remote access managed entirely with secure solutions over encrypted channels (e.g., campus VPN)?

Is file encryption in use on all mobile devices that store or transmit patient health information or other confidential information?

Is encryption used on all outbound transmissions of patient health information or other confidential information?

Software Updates and Patches

Are the latest patches and updates applied to your system as soon as they are made available?

Unnecessary Services

Have you disabled unnecessary services on your computer?

Comments:

**OAAIS Enterprise Information Security
Security Awareness, Training & Education (SATE) Program**

<http://security.ucsf.edu>
(Manager Checklist) 11/2007