University of California
San Francisco
advancing health worldwide

UCSF Minimum Security Standards Checklist

All systems used for conducting UCSF business should follow UCSF Minimum Security Standards to be in compliance with UCSF Policy 650-16 and UCOP's IS-3 Policy governing Electronic Information Security. This checklist can be used to determine, and/or document, the compensating controls necessary to minimize information security risks as outlined in the UCSF Minimum Security Standards. Any item(s) marked "No", may require filing for a Security Exception.

For any questions about this form, or any specific item(s) below, please email IT-Questions@ucsf.edu.

Physical Security

☐ Yes ☐ No Are devices located in locked areas or otherwise physically secured when left unattended?

☐ Yes ☐ No Are all devices/systems set to auto-lock requiring a password for access after a twenty-minute (maximum) period of inactivity and when the screen saver is activated?

System Security

☐ Yes ☐ No Do all systems enforce password guidelines as outline in the UCSF Enterprise Password Standard?
+ Users are required to change pre-assigned passwords immediately
+ All default passwords set by the vendor/manufacturer have been changed and are changed on a regular basis (e.g. quarterly, yearly, and/or everytime an employee leaves the organizations)

☐ Yes ☐ No Is anti-virus/anti-malware software, such as Symantec Endpoint Protection, installed and enabled, with virus definitions kept up-to-date and recent on all systems?

☐ Yes ☐ No Are all systems/applications still supported by their vendor/developer and kept up-to-date with the most recent applicable security patches?

☐ Yes ☐ No Do all the systems have unnecessary services disabled?

Network Security

☐ Yes ☐ No Do all devices have a host-based (software) firewall, such as Symantec Endpoint Protection, installed and enabled?

☐ Yes ☐ No Are all servers, and/or devices, that handle sensitive, protected or confidential information on a segregated network and protected by a network hardware firewall and/or IPS?

Securing Sensitive, Protected, or Confidential Information

☐ Yes ☐ No Are all systems and devices (desktops, laptops, and mobile devices) encrypted with a solution, such as PGP or DDPE, that is able to provide proof of encryption in the event of loss or theft?

☐ Yes ☐ No Is whole disk encryption used on all systems storing confidential information like ePHI or PII?

☐ Yes ☐ No Do all users in your department know how to use Secure Email to ensure that all emails containing protected health information or other confidential information are encrypted?

☐ Yes ☐ No Is every single mobile device encrypted and configured to require a PIN lock? (ActiveSync will automatically configure these options)

☐ Yes ☐ No Is remote access into UCSF resources from non-UCSF networks, managed entirely through encrypted channels over a secure solution, namely UCSF VPN?

☐ Yes ☐ No Is transmission of restricted information over non-UCSF networks encrypted (e.g. using SSL Certificates across https)?

☐ Yes ☐ No Are all forms of authentication using adequate encryption to protect against unauthorized access to login credentials, such as user accounts and passwords?

☐ Yes ☐ No Is restricted information transmitted *only when necessary*?

Full Name: _____ Department: _____

Email: _____ Signature/Date: _____

information technology