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 Addendum B 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 and/or physically secured (e.g. w/ cable lock) when left unattended?

□Yes □No Are all devices and systems set to auto-lock requiring a password for access after a reasonable period of inactivity (20 minutes maximum) and when the screen saver is activated?

Application and System Security

□Yes □No Do all systems enforce password guidelines as outlined 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 every time an employee leaves the organizations)

□Yes □No Do privileged administrator accounts have 15+ character passphrases that are reset every 90 days?

□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? (Legacy or End-of-Life Systems should mark this 'No')

□Yes □No Do all web site and application developers follow secure coding best practices and conduct periodic vulnerability assessments on their web sites and applications?

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

□Yes □No Are all network-capable systems (servers, desktops, laptops, network gear, printers, etc) inventoried into the enterprise configuration management database (CMDB) via BigFix or manual registration?

Network Security

□Yes □No Do all devices have a software firewall, such as Symantec Endpoint Protection, installed and enabled?

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

□Yes □No Do all computers have system management software installed?

□Yes □No Are all servers and devices able to be scanned on the network for vulnerabilities?

Securing Sensitive and/or Protected Information

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

□Yes □No Do all systems and devices have their UCOP protection level classification set in the enterprise CMDB?

□Yes □No Is restricted data (like ePHI, PII, or PCI) encrypted wherever it is stored, including backups and removable drives?

□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 and screen timeout? (ActiveSync will configure these options automatically)

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

□Yes □No Do vendors adhere to 3rd Party Remote Access Standards when accessing UCSF resources remotely?

□Yes □No Is transmission of restricted data to non-UCSF networks encrypted (e.g. using sftp, or SSL Certs on https)?

□Yes □No Are all forms of authentication encrypted to protect against unauthorized access to login credentials?

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

Full Name:______________________________ Department:______________________________

Email:______________________________ Signature/Date:______________________________

Information
Technology