Image not found
https://it.ucsf.edu/sites/it.ucsf.edu/themes/custom/it_new/logo.png
it.ucsf.edu
Published on *it.ucsf.edu* (https://it.ucsf.edu)

UCSF Minimum Security Standards for Electronic Information Resources

Esther Silver on January 28, 2020

Policy Type

Standard

Effective Date: December 2007, Updated November 2018

Contents

10. Device Encryption
11. Encrypted Authentication
12. Passwords
13. Software Patch Updates
14. Application and Website Security
15. Enterprise Vulnerability Management

Purpose

UCSF Policy 650-16, Addendum B, defines a requirement for Minimum Security Standards for Electronic Information Resources (EIR). This document is a living document that defines the UCSF Minimum Security Standards that all campus EIRs must comply with.

Overview and Scope

These standards apply to all departments within UCSF and the UCSF Medical Center.

Non-UCSF devices, including personal computing devices, are expected to meet these standards when used to connect to the UCSF network. For example, a personal computer that accesses the UCSF network through a VPN connection would be expected to meet these standards. Additionally, non-UCSF devices are expected to meet these standards when used to conduct UCSF business, including storing or processing UCSF information.

The minimum standards in this document are reviewed, updated for applicability, and approved by the Information Security Committee (ISC) at least once a year or more often as determined by Security & Policy (S&P).

UCOP protection level classifications (PLC) are defined here [1]

Exception from Minimum Security Standards

Individuals who believe that their devices or applications are unable to meet UCSF?s Minimum Security Standards must apply for a yearly exception by completing and digitally signing the online form linked below. Upon receiving the completed form with signatures from the individual's department leadership, IT Security will contact you for a consultation. After this consultation the University's Information Security Officer will respond to your request.

Instruction for filling out Security Exception Request Form (UCSF MyAccess Login required) [2]

Exception Requests Covering Legacy Systems

If granted, exception requests for an operating system that is no longer supported by the vendor will be for 12 months from the date of approval. At each renewal you must document the steps you are taking to mitigate the risk to the system and to UCSF. Failure to renew an exception may result in disconnection from UCSF's network.

For systems which access to or which store ePHI, departments are advised that this exception documentation and controls should be considered carefully to remain compliant with HIPAA section § 164.308(a)(1)(ii)(B), which requires UCSF to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Controls are countermeasures to help avoid or minimize security risks. These controls are generally implemented as technologies not directly associated with the system seeking exception from UCSF's Minimum Security Standards.

Compatibility Exemptions

Systems incompatible with or unsupported by the UCSF-specific tools will be exempted from that requirement(s) of the Minimum Security Standards. Any Compatibility Exemption will be listed by security application and OS in the Security 2.0 faq [3].

Minimum Security Standards

System Inventory and Protection Level Classifications

Systems must be inventoried as a configuration item in the enterprise configuration management database (CMDB); this includes but is not limited to: servers, systems, endpoints, networking devices, printers. This applies to all devices used for UCSF business. Any changes to the system throughout its lifecycle must be recorded in the enterprise CMDB.

Devices meeting the System Management Agent standard are automatically inventoried. Devices that are incompatible or not supported by the System Management standards, can be inventoried and/or their registration updated using the ServiceNow CMDB [4].

Additionally, systems must have their protection level classification set in the enterprise CMDB. UCOP protection level classifications are defined here [1].

Transmission of Restricted Information

Restricted and Sensitive Information (UCOP P4 and P3 data) that is transmitted over non-UCSF networks must be encrypted. Restricted Information includes, but is not limited to, ePHI and personal information such as Social Security numbers.

Transmit P4 and P3 data only when necessary.

Email

All email that contains electronic Protected Health Information (ePHI) or other Restricted Information must be encrypted if it is addressed outside the UCSF network environment. An existing service is available to accommodate encrypted email: Secure Email Procedure [5]

Non-UCSF or 3rd party email services are not approved for use by faculty, staff, or students for conducting UCSF business.

Physical Security

Unauthorized physical access to an unattended device (including mobile devices) can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. Whenever possible and appropriate, devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 20 minutes.

Computing devices that are left unattended must be located in locked areas or otherwise physically secured (e.g., with a cable lock).

System Management Agent

In order to inventory computers and enable basic security compliance, users must install system management software provided by IT. This applies to both UCSF-owned and non-UCSF-owned endpoints.

The system management software uses BigFix and is available through the UCSF IT Software Download page [6].

Network Access Control (NAC)

In order to identify computers connected to the UCSF network, assess endpoint security compliance, and prevent unauthorized computers from connecting to the UCSF network, users must install system management software provided by IT. This applies to both UCSF-owned and non-UCSF-owned endpoints.

The Network Access Control software, SecureConnector, is available through the UCSF IT Software Download page [6]. (Note: Review Service Page details for additional requirements and supported platforms).

Anti-Virus Software

Anti-virus software must be active with current anti-virus signatures on computing devices connected to the network including laptop computers, desktop computers, and servers, except where there are significant compensating controls that would prevent virus infiltration.

IT currently has a contract with Symantec to provide anti-virus software and is available through the UCSF IT Software Download page [6].

Host-Based Firewall Software

Firewalls that run on desktops, laptops and servers are often referred to as host-based and/or personal firewalls. Host-based firewall software (if available for the platform) must be running and configured on networked computing devices, including laptop computers, desktop computers, and servers. While the use of departmental network firewalls is encouraged, they do not necessarily obviate the need for host-based firewalls.

IT currently has a contract with Symantec that provides a host-based firewall solution and is available through the UCSF IT Software Download page [6].

Security Endpoint Detection and Response Agent (EDR)

In order to provide advanced protection monitoring and response capabilities, users must install the Security Endpoint Detection and Response agent provided by IT. This applies to both UCSF-owned and non-UCSF-owned endpoints.

The Security Endpoint Detection and Response agent is available through the UCSF IT Software Download page [6] as bundled with system management software (BigFix). (Note: Review Service Page details for additional requirements and supported platforms)

Device Encryption

Given the prevalence of restricted data in the UCSF environment, all endpoints (desktops, laptops, and mobile devices including smartphones and tablets) used for UCSF business must be encrypted. This applies to both UCSF-owned and non-UCSF-owned endpoints.

Servers that store or process restricted information must be encrypted or have compensating security controls, such as those found in UCSF data centers.
IT provides encryption software for laptops and desktops. How to Encrypt Your Computer [7]

Mobile devices must be connected to the UCSF Exchange email server with ActiveSync, which enforces the required security settings. More information regarding connecting your smartphone can be found at http://it.ucsf.edu/services/email-mobile-access/tutorial/iphone-email-configuration

[8].

Those who believe they need an exception to this device encryption standard due to a hardware or software incompatibility must submit a computer encryption waiver (http://it.ucsf.edu/how_do/request-device-encryption-waiver [9]).

Store restricted information only when necessary.

Encrypted Authentication

All forms of authentication must use adequate encryption to protect against unauthorized access to login credentials, such as user accounts and passwords. Use of unencrypted authentication is prohibited.

Passwords

Campus electronic communication systems or services must identify users and authorize access by means of passwords or other secure authentication processes. Shared-access systems must enforce the Unified UCSF Enterprise Password Standard [10] whenever possible. Shared-access systems must, whenever possible and appropriate, require that users change any pre-assigned passwords immediately upon initial access to the account.

All default passwords for access to network-accessible devices must be modified. Passwords used by system administrators for their personal access to a service or device must not be the same as those used for privileged access to any service or device.

Privileged administrator accounts with access to sensitive Windows systems should use passphrases that are 15 or more characters in length and meet the Unified UCSF Enterprise Password Standard [10]. Passphrases should be reset at least every 90 days.

Software Patch Updates

Networked computing devices must be kept updated with the most recent applicable security patches. Departments should document and implement a process to apply security patches in a timely fashion. Exceptions may be made for patches that compromise the usability of critical applications; these exceptions should be documented.

Application and Website Security

Application and web site owners are responsible to ensure that applications and sites are secure, and must conduct periodic vulnerability assessments of these applications and sites. More information regarding secure coding best practices and vulnerability scanning services can be found here. [11]

Enterprise Vulnerability Management

Systems connected to the UCSF network are subject to vulnerability scanning on a routine basis by IT Security to identify vulnerabilities. System owners must ensure that their devices do not inhibit the enterprise vulnerability management tool to scan their systems.

All devices connected to the UCSF network must meet the remediation timelines associated with the vulnerability severity and protection level classification. Remediation timeline begins when a vulnerability is publicly announced. Major vulnerability exploits can lead to an adjustment of vulnerability remediation timelines and priorities. These out-of-band instances will be communicated by IT Security.

Vulnerability Classification				
Protection Level Classification		Critical	High	Medium
	P4	7 days	14 days	21days
	P3	14 days	14 days	21days
	P2	21 days	21 days	30 days
	P1	21 days	30 days	30 days

Minimum Security Standards Checklist

The following checklist can be used to determine, and/or document, the compensating controls necessary to minimize information security risks as outlined in the above UCSF Minimum Security Standards.

https://wiki.library.ucsf.edu/display/ITSI/UCSF+Minimum+Security+Standards+Checklist (UCSF MyAccess Login required) [12]

device_encryption_waiver.pdf [13]
image001_2.png [14]

Suggest an IT Improvement | © UC Regents

*/ //-->

Source URL: https://it.ucsf.edu/policies/ucsf-minimum-security-standards-electronic-information-resources

Links
[1] https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html
[2] https://wiki.library.ucsf.edu/display/ITSI/IT+Security+Exception+Request+Process
[3] https://wiki.library.ucsf.edu/display/ITS/Security+2.0+FAQ
[4] http://itsm.ucsf.edu/service-asset-and-configuration-management
[5] https://it.ucsf.edu/services/secure-email
[6] https://software.ucsf.edu/
[7] https://it.ucsf.edu/encrypt
[8] https://it.ucsf.edu/services/email-mobile-access/tutorial/iphone-email-configuration
[9] https://it.ucsf.edu/how_do/request-device-encryption-waiver
[10] https://it.ucsf.edu/policies/unified-ucsf-enterprise-password-standard-0
[11] https://it.ucsf.edu/policies/application-and-web-site-security
[12] https://wiki.library.ucsf.edu/display/ITSI/UCSF+Minimum+Security+Standards+Checklist
[13] https://it.ucsf.edu/sites/it.ucsf.edu/files/device_encryption_waiver.pdf
[14] https://it.ucsf.edu/sites/it.ucsf.edu/files/image001_2_2.png