Device Encryption

Marc Lowe on January 30, 2020

What is encryption? Why do I need it?

Encryption is the process of encoding information so that only authorized persons can read it. It is used to protect confidential and legally protected data. If an unencrypted laptop, tablet, smartphone, or other device is lost or stolen, and if it contained legally protected information, you or the University might be held liable for damages, you could be sent to prison, or the University could take corrective action against you.

The UCSF Minimum Security Standards state, ?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." UCSF Minimum Security Standards for Electronic Information Resources [1]

What devices need to be encrypted?

Almost all devices used for UCSF business, research, or studies.

This is true:

- whether or not they are owned by UCSF
- whether or not the device currently contains legally protected data
- whether or not the device is likely to contain legally protected data in the future

What devices do not need to be encrypted?

- Devices that are *never* used for UCSF business, research, or studies.

- Devices that are used for UCSF business, research, or studies and which do not contain legally protected data and which are incompatible with encryption solutions provided by UCSF IT. These devices don?t need to be encrypted, but you must complete and submit the Request device encryption waiver [2] for each one.

You must report lost or stolen devices.

You are legally obligated to report a lost or stolen device [3] used for UCSF business, research, or studies:

- whether or not UCSF owns it
- whether or not it contains legally protected data
- whether or not you know if it contains legally protected data
- whether or not it was encrypted

Devices include: desktop computers, laptop computers, tablet computers, smartphones, cdroms, dvdroms, floppy disks, and any media that can store data.

Encrypting computers

Including desktops and laptops for Mac and Windows:

How to Encrypt Your Computer [4]

How To Determine Your Computer Encryption Status [5]

Encrypting smartphones and tablets

iPhone and iPad (iOS)	• If you have an iPhone 3GS or later, your iPhone includes hardware encryption. If you use it for UCSF business, research, or studies, complete the iPhone ActiveSync Email Configuration [6]. This satisfies the UCSF encryption requirement because it enforces our policy of requiring a passcode for the device. • All iPads include hardware encryption. If you use yours for UCSF business, research, or studies, complete the iPad Email Configuration [7]. This satisfies the UCSF encryption requirement because doing so enforces our policy of requiring a passcode for the device. • iPhone 3G and earlier models may not be used for UCSF business, research, or studies.

Android, Microsoft, & BlackBerry

Please follow the instructions for setting up your UCSF email on your phone; that will also ensure your phone is encrypted.

- enable encryption android [8]
- enable encryption microsoft [9]
- enable encryption blackberry [10]

If needed, contact the IT Service Desk [11] for help.

Encrypting USB drives, CDroms, DVDroms, floppy disks, etc.

Do **both** of the following:

Move the data to an encrypted device

Copy the data to your encrypted desktop or laptop computer. Or:

1. Buy an encrypted portable storage device. (See Buy Recommended Security Products? [12])
2. Copy the data from the original device to the new device.

Destroy or securely remove the data from the original device

1. If you can securely erase the original device, you may use it for things other than UCSF business, research, or studies.
2. If you cannot securely erase the original device, send it to be securely destroyed. See Drive, Tape, and Data Destruction [13].

Other useful Encryption Links:

How To Determine Your Computer Encryption Status [5]

Dell Data Protection Encryption (DDPE) [14]

DDPE Frequently Asked Questions (FAQ) [15]

Encryption Project [16]

Get help

Contact the IT Service Desk [11].

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

Site Login Site Index

Suggest an IT Improvement | © UC Regents

*/ //-->

Source URL: https://it.ucsf.edu/encryption

Links
[1] https://it.ucsf.edu/policies/ucsf-minimum-security-standards-electronic-information-resources
[2] https://it.ucsf.edu/how_do/request-device-encryption-waiver
[3] https://it.ucsf.edu/how_do/report-lost-or-stolen-mobile-device
[4] https://it.ucsf.edu/encrypt
[5] https://it.ucsf.edu/how_do/how-determine-your-computer-encryption-status
[6] https://it.ucsf.edu/services/email-online-mobile/tutorial/iphone-activesync-email-online-settings
[7] https://it.ucsf.edu/services/email-mobile-access/tutorial/ipad-email-configuration
[8] https://it.ucsf.edu/services/email-mobile-access/tutorial/activesync-settings-android
[9] https://it.ucsf.edu/services/email-mobile-access/tutorial/windows-mobile-email-sync-settings
[10] https://it.ucsf.edu/services/email-mobile-access/tutorial/blackberry-10-os-activesync-configuration
[11] https://it.ucsf.edu/
[12] https://it.ucsf.edu/how_do/recommended-security-products
[13] https://it.ucsf.edu/services/drive-tape-and-data-destruction
[14] https://it.ucsf.edu/services/dell-data-protection-encryption-ddpe
[15] https://it.ucsf.edu/services/dell-data-protection-encryption-ddpe/additional/ddpe-frequently-asked-questions-faq
[16] https://it.ucsf.edu/projects/encryption-project