DEFINITIONS

"Encryption" is a technology that protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people.

"Full Disk Encryption" or "Whole Disk Encyrption" encrypts all data on a system, including files, folders and the operating system.

STANDARD

1) The only full disk encryption methods for workstations and laptops that are approved for use are listed below:
   a) Checkpoint full disk encryption

      ISS and DGIT will require Checkpoint to be installed on all new Windows systems they support as of December 31, 2017.

   b) Symantec PGP whole disk encryption

      Note, all new Windows systems should be encrypted with Checkpoint.

   c) Microsoft BitLocker full disk encryption

      Note, all new Windows systems supported by ISS and DGIT should be encrypted with Checkpoint.

   d) Apple FileVault full disk encryption
2) For workstations and laptops encrypted with the built-in encryption solutions BitLocker or File Vault:
   a) Owners or IT must enter the device into the DGIT encryption registration database by following the instructions at the link below:

      https://inventory.dgsom.ucla.edu/inventory/self-eua

   b) The owner must arrange for secure back up of the encryption key to allow for data recovery if the password is forgotten.
3) For non-UCLA owned workstations on which the users never store University Business documents, even temporarily, and for which the only University Business use of the workstation is for a function listed below may be exempted from the encryption requirement of HS Policy No. 9453C, "Device Encryption:"
   a) CareConnect remote access
   b) Outlook web access
   c) Windows remote desktop for Windows

TECHNICAL REQUIREMENTS

1) All hard drives installed in workstations and laptops must be encrypted using full-disk encryption with Advanced Encryption Standard (AES) with a key length of 256 bits.
2) All removable media must be encrypted using full-disk encryption with Advanced Encryption Standard (AES) with a key length of at least 128 bits. Encryption ciphers should be FIPS 140-2 validated.

QUESTIONS

1) Find answers for mobile device encryption questions on the Frequently Asked Questions page at the link below:

   https://inventory.dgsom.ucla.edu/encryption/faq

2) Visit IT Connect in the CHS Café Med for walk-in encryption support:

   http://medschool.ucla.edu/it-connect

3) Your IT Support Group can also help with any device encryption questions you may have.
4) If you have questions about this Standard, please contact the Office of Compliance Services – Information Security (InfoSecAll@mednet.ucla.edu)

REFERENCES

HS Policy No. 9453C, "*Device Encryption*"

CONTACT

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Created Date: July 18, 2017
Revised: 11/20/17