Whole disk encryption

Laptops carrying sensitive data (as defined by the Duke University data classification standard) must be encrypted according to the Duke University ITSO technical standards [1] (NetID required). It is also our strong recommendation that all laptops be encrypted. Computers in Duke Health are subject to different policies regarding encryption; see the "Duke Medicine PGP User How-To [2]" Duke KnowledgeBase article for details.

Windows computers should use Windows BitLocker Drive Encryption [3]. Apple OS X computers should use Apple's FileVault 2 [4].

For computers managed by end users

Users that are not supported by Duke IT staff should follow the instructions linked below:

- To enable Windows BitLocker, see the "How to Enable Windows BitLocker [5]" Duke KnowledgeBase article
- To enable Apple OS X FileVault 2, see the "Enabling FileVault 2 in OS X [6]" Duke KnowledgeBase article.

These instructions are also recommended for individuals to use on their personally-owned computers.

For computers managed by Duke IT staff

Duke IT staff should follow the same processes linked above, but additional steps must be taken beforehand in order to ensure that the recovery key is recorded in a central location (i.e. "key escrow").

- To escrow Windows BitLocker recovery information in Active Directory, see the "How to Store BitLocker Recovery Information in Active Directory [7]" Duke KnowledgeBase article
- To escrow Apple OS X FileVault 2 recovery information, enroll the computer in the Duke University Casper instance (send an e-mail to casperadmins@duke.edu [8] for more information) and then refer to one of the JAMF guides on "Administering FileVault 2 with the Casper Suite [9]".
Source URL: https://security.duke.edu/services/whole-disk-encryption

Links
[8] mailto:casperadmins@duke.edu