NYSPI Endpoint Encryption

To address NYS and NYSPI-specific agreements and requirements, all workstations hosting NYSPI data or on the NYSPI network must be encrypted. Devices owned and supported by PsyIT will be encrypted by PsyIT. If your device is not currently encrypted but is supported by PsyIT, please enter a service desk ticket to schedule that setup.

For individuals or groups supporting their own workstations:

Apple Mac systems can be encrypted using the native FileVault2 solution, as documented at https://support.apple.com/en-us/HT204837. NYSPI-specific recommended procedures can also be found at http://psyit.nyspi.org/Docs/Procedures/NYSPIMacEncryptionProcedure.pdf

Windows systems should be encrypted using Microsoft Bitlocker unless a third-party whole-disk encryption solution is installed and approved by the NYSPI Chief Information Security Officer. Instructions for configuring Bitlocker can be found at http://www.cumc.columbia.edu/it/howto/encrypt/bitlocker.html or https://uit.stanford.edu/service/encryption/wholedisk/bitlocker . Bitlocker should be configured to use AES-256-bit encryption.

Users of Linux or other operating systems should refer to the appropriate operating system documents for implementing encryption.

Additional guidance on encryption requirements of both data and devices can be found in the NYS Encryption Standard at http://on.ny.gov/2bSYU3T.

Questions or requests for exceptions can be sent via a service desk ticket or via e-mail to PsyIT-Admin@nyspi.columbia.edu