Information Security: Whole Disk Encryption

Faculty and staff members who work with sensitive data at Lehigh, such as confidential student personal or health records, staff personal or employment data (including performance appraisals), and employee identification numbers, should store this information securely on their workstation, laptop, or in a secure location on a network. Client Services recommends that sensitive data be stored on a secure network location (such as a user's H: Drive). In cases where sensitive data needs to be stored on a workstation or laptop, it is recommended that Whole Disk Encryption be used. Whole Disk Encryption (WDE) is the highest level of encryption and is recommended for users who need to secure an entire hard disk or external storage device. This type of encryption is HIGHLY recommended by LTS because it secures the entire hard disk so users do not need to know where sensitive data files are stored.

Windows 7 Enterprise and Ultimate versions (Bitlocker) and the newer versions of the Macintosh operating system (FileVault) have WDE software built into the operating system. The following operating systems can be encrypted using WDE:

- Windows 10 (Enterprise and Ultimate/Pro Versions only) Bitlocker
- Macintosh FileVault (OSX Lion and newer)

Students who want to encrypt their computer or files, please see http://www.lehigh.edu/stars.

Encrypting a Computer Using WDE

For Faculty/Staff - please contact your department computing consultant by entering a self-service Jira ticket at http://www.lehigh.edu/help or call the Help Desk at 610-758-HELP (4357). Faculty/Staff are able to encrypt their computers; however, they are encouraged to have an LTS staff member perform the encryption so encryption keys are properly recorded and University computers can be accessed in the event of an emergency.

Retrieving a recovery key if locked out of a system

Windows computers encrypted using Bitlocker have their encryption keys automatically backed up. This backup enables a user or client services staff member to unlock a computer if for some reason a computer is locked by Bitlocker. A computer is locked sometimes when Bitlocker senses a potential security risk with your system - this seldom happens, but in the event it does, there is a self service recovery tool available. Please click on the following link to access the Bitlocker self service recovery tool.

For Windows PCs in the "AD" domain:

- http://www.lehigh.edu/go/bitlockerhelp

For Windows PCs in Intune:

- How to get your Bitlocker Recovery Key from an Intune PC

Note: In order to retrieve your key, you must have another means to access this tool other than the primary computer that is locked - such as a smartphone or second computer. If you do not have this, please contact your department computing consultant or the Help Desk at 8-HELP (4357).