Office of the Chief Information Security Officer
Risk Advisory: Whole Disk Encryption

BACKGROUND

It is important to protect the availability, confidentiality, and integrity of critical information assets wherever they are stored, and whether they reside on UW-owned or personal computers and devices. If you lose physical possession of your computer, whole disk encryption can protect your data against falling into the wrong hands. Whole disk encryption has limits. It cannot protect your data when your computer is powered on and unlocked, nor can it protect your data from network attack or surveillance. Furthermore, if encryption is not properly installed and carefully managed, you may irrecoverably lose access to your data. Therefore, while whole disk encryption is an essential security safeguard, it is very important to exercise best practices for the protection to be effective.

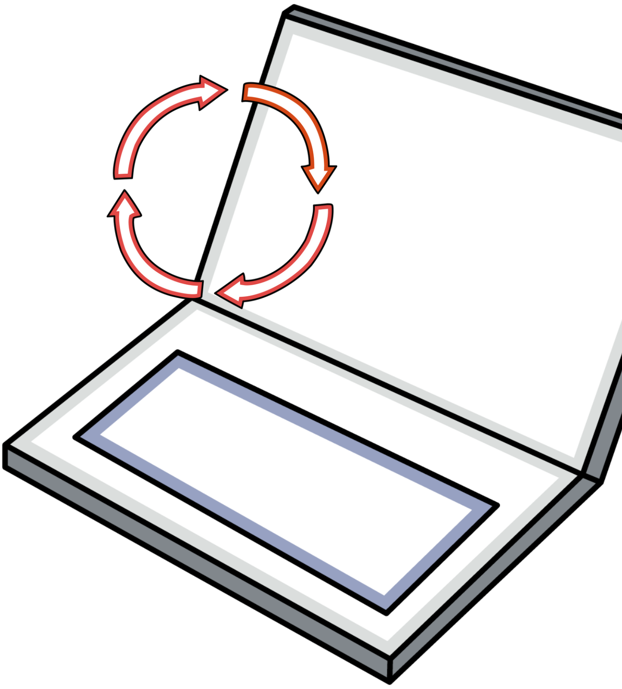
BEST PRACTICES

Before attempting to encrypt the hard drive:

- Back up your data to external media
- Run a disk check utility and allow the utility to repair errors

Plan how you will administer encryption effectively:

- Your password/passphrase is potentially the weakest link – choose a good one
- Store your recovery key in a safe place – other than on your computer
- If your University organization has support personnel responsible for managing the inventory of desktops and laptops, work with them to document the fact that the device is encrypted, and how the recovery keys are managed



TIPS

If you are purchasing a new mobile computer through eProcurement, you can add **BitLocker** (Windows only) encryption during the purchase process. CDWG will encrypt the hard drive for you, but you will still need to back up your encryption key.

Office of the CISO, May 2016

Plan how you will use encryption effectively:

- Enable a screensaver/auto-lock and require a password/pin to unlock
- Manually lock your screen if you’re going to be away from your computer
- Power off your computer completely (do not just suspend it) when you think it could be at risk of falling into someone else’s hands
- Consider using a cable lock to secure your computer
- Always maintain physical control of your mobile computer

RESOURCES

Windows Guidance

MAC Guidance