Laptop Security and Encryption Standard and Guidelines

Laptop Security best practices, as stated in the University Encryption Procedure (currently under development and awaiting approval), are currently defined as follows:

The use of any sensitive information on mobile computing devices must be avoided unless absolutely necessary. Sensitive information should be stored on a secured system at the University and accessed via a secure and approved University remote access connection from the remote computer to that system. A remote desktop/terminal service deployment for instance, provides for secure remote access connections. Remote access of University information technology resources must not leave any residual or cached sensitive information on the local machine.

The University community is responsible for safeguarding University information and has the responsibility to uphold information privacy and security on all University mobile computing devices.

This responsibility to safeguard University information also extends to personal, external, and non-University computing devices that store University sensitive information.

MINIMUM REQUIREMENTS

In situations where it is not possible to avoid the use of sensitive information on a mobile computing device or where there is any doubt about the nature of the data on a mobile computing device, then the device must be secured to the following minimal baseline:

a) Laptops and other mobile computing devices must run a current, fully patched, and modern operating system at all times.

b) Users must store documents on laptops in a single specific area only (such as a home folder or directory).

c) The contents of the disk storage area specified in b) must be securely encrypted.

d) Laptops and other mobile computing devices must be configured to ask for a password after any period of inactivity, including after resuming from suspend/standby/sleep/hibernate status and on operating system start-up.

Additional laptop and mobile computing security measures include:

a) Personal digital assistant (PDA) devices must have the ability to conduct a remote kill.

b) Laptops and other mobile computing devices must follow electronic media disposition and secure wipe in accordance with the electronic media disposition guidelines.

c) Physical protection controls must be used, such as laptop cable locks and securely storing mobile devices in transit and in locked areas/compartment when not in use.

d) Wireless security best practices must be followed when connecting to information technology resources through WiFi.

e) Strong authentication should be considered if there is an approved and justified business need to access University of Alberta sensitive information using a laptop or other mobile computing device.
Laptop Encryption Deployment Guidance For System Administrators

The current best practice mechanisms for secure, software-based disk encryption as described in practice 2C are the following:

**Microsoft Windows:** Configure BitLocker to encrypt all fixed disk drives

**Apple**
- Mac OS X 10.6: Configure FileVault to encrypt all users’ home folders
- Mac OS X 10.7: Configure FileVault 2 to encrypt laptop fixed disk

**Linux:** Configure TrueCrypt (Open Source software) to encrypt laptop fixed disk

Different mechanisms may be acceptable to use on other operating systems. If a platform not listed here is **not** capable of encrypting the stored documents area, it **must not** be used to store sensitive information (it may be used for secure remote access to a system as in section 1).

5) A deployment plan for disk encryption must be defined and approved in a unit prior to encrypting user systems or data. Minimally, this plan should cover:
   - Identification of affected assets;
   - Definition of established data backup processes
   - Definition of encrypted data recovery management process
   - Definition of encryption deployment process
   - Testing of encryption deployment
   - Reporting on encryption process status

Recovery Management

See the University’s Recovery Management Guidelines:  

Encryption Instructions

See the University’s Encryption Website for instructions: [http://www.vpit.ualberta.ca/encryption/](http://www.vpit.ualberta.ca/encryption/)

---

1Note that BitLocker is only available for the Ultimate and Enterprise editions of Windows 7 and Vista - it is highly recommended that Windows XP **not** be used on laptops requiring data encryption.
References: