Encryption at MIT

Encryption at MIT

This article addresses the availability and use of encryption tools at MIT. The listed tools and following questions and answers attempt to provide a clarification of practices around encryption.

Recommended Tools

Windows	Mac
	
BitLocker: Learn more	FileVault: Learn more
Runs on Windows Vista and Windows 7 (Ultimate and Enterprise), Windows 8 and later (Pro and Enterprise), and Windows Server 2008 and later.	Runs on Mac OS X 10.7 and higher.

IS&T provides assistance for these tools through the IS&T Service Desk.

What is encryption?

Encryption is the conversion of data into a form called ciphertext, that cannot easily be read by unauthorized people. There are different forms of encryption, including wireless encryption, whole disk encryption and file encryption. All references to encryption in this article refer to whole disk encryption (WDE), which has to do with the encryption of a computer disk or flash drive.

When is encryption recommended?

The main incentive for using encryption is when personal information exists on a disk or computerized device. In fact, Massachusetts regulations setting forth Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR §17), and in support of the laws for protecting consumer data, mention that encryption is required for all personal information stored on laptops or other portable devices.

Because desktops can also be stolen, we recommend encryption on those machines as well, if they contain sensitive personal information.

How much time is involved in implementing encryption on a machine?

The time it takes to encrypt a disk or drive depends on its size and its contents. In general, you may need to put several hours aside to allow a disk to fully encrypt the data contained on it.

Will I notice any difference in performance when I enable encryption?

No. While the computer is turned on and you are logged in, the encryption feature is not enabled. The disk is only encrypted when the computer is off or you are logged off.

What are the risks with encryption?

The primary risk when using encryption is losing the pass code used to access the key to the encrypted disk:

- If you use http://kb.mit.edu/confluence/x/BIgBCQBitLocker distributed by Microsoft in the OS; and are in the Win domain, you can recover

the key by contacting the IS&T Help Desk.
- For FileVault users, you can store your key yourself or with Apple. Note that departments, labs or centers may have their own policy for storing encryption keys.
- For mobile devices, recovery of the key to unlock a phone or tablet may be difficult to impossible; contact the IS&T Help Desk or the vendor for support.

What if I want to use something other than BitLocker or FileVault 2 on my computer?

IS&T only provides support for BitLocker and FileVault. IS&T technicians may attempt to assist you with other encryption software tools, but for full support contact the software vendor.

See Also

- Encryption Landing Page