


# Secure Data Encryption on Portable Storage Devices

The LCTCS Office of Information Technology policy on portable device data security states:

All sensitive data that is stored on agency approved portable storage devices (Notebook PCs, USB thumb drives, USB hard drives, CDs, DVDs, diskettes, PDAs, etc.) that are removed from the state premises must be encrypted and consistent with OIT STD 023 (Encryption Standard). -- [IT-POL-014](#) 

So, what can you do to protect data that you have in your possession?

First, let's start with some possible sensitive data you might have and how you can protect it and yourself. Sensitive data about you, students, faculty members, and employees can live anywhere that you store digital information including a desktop computer, a laptop, a PDA, a flash drive, or other recordable media.

Student data (grades, SSNs, etc.) also needs to be protected and treated as sensitive data. While it's convenient to copy files onto portable/mobile devices and media, what information do you really need to be with you at all times? Theft of portable devices is a very serious problem and having data stolen is becoming a large problem too.

## What is Encryption?

Encryption is a means to encode data. The purpose of encryption is concealment, or more specifically, security and confidentiality. Things like digital signatures are often confused with encryption, but they are not concerned with concealment, rather they deal with integrity and authenticity, or more simply, verifying a sender and that the contents of a message have not been changed.

E-mail sent without encryption is like a postcard; others can see the contents if they use special tools to pry. With the use of encryption, only the recipient of the message can open and view the contents of the e-mail. It's like putting it in an envelope and sending it by registered mail. Data other than e-mail can also be stored encrypted so that others cannot easily see its contents.

## Why should I care about Encryption?

Typically, encryption is not needed for standard, day-to-day activities. In order to determine if you have digital data that needs to be encrypted, here are some basic guidelines that can be used to determine if encryption is worth implementing. If you answer yes to any of these basic questions, then you should to consider using some form of encryption.

- Is my data sensitive? If so, how? If your data contains information that is sensitive only to you, and its disclosure does not impact other people's privacy, then is it worth it to encrypt data? Conversely, if disclosure would impact other people's privacy, then you should definitely look at encryption. (Personal information can be defined as an individual's name in combination with the individual's social security number; driver's license or campus-wide identification number; or account number or creditor debit card with security codes or passwords.)
- Are there already safeguards in place to protect my data? If your data is not portable, nor publicly accessible, then physical compromise is likely the only real threat. Is this threat enough to warrant encryption of data? If your data is mobile (i.e. on a laptop), then physical theft or compromise is a very real concern.
- Are there policies or laws currently in place governing the data you have ([FERPA](#), HIPAA, BPCC regulations)? If so, what are those requirements and have you made due diligence in meeting them?

## How can I encrypt data?

There are so many different methods, standards, and algorithms used to encrypt data that their discussion falls well outside of this document. Instead, a couple of very basic methods should cover most needs.

- **E-mail** - The most common method for encrypting e-mail is by using software like the GNU Privacy Guard (GnuPG, available at <http://www.gnupg.org>). GnuPG is free and works on most operating systems and hardware platforms. Setup and use of the program are very well-documented on the GnuPG website.
- **Hard Drive** - Please remember that it is never a good idea to encrypt your entire hard drive. Rather, pick and choose which folders should be encrypted. Also be aware that if you cannot unlock the files due to a hard drive failure or other issue, this data may be lost. Caution: encryption uses keys, which, like passwords, can be lost or forgotten.
  - **PC** - Windows XP supports file encryption natively, and you can pick and choose what parts of your hard drive to encrypt. A good step by step guide can be found at <http://www.practicalpc.co.uk/computing/windows/xpencrypt1.htm>.

Also, an encryption application called TrueCrypt is free and available for [download](#) and installation at [TrueCrypt.org](http://TrueCrypt.org). On the TrueCrypt [documentation](#) page, scroll down and click on "Beginner's Tutorial". **NOTE: If you print the Beginner's Tutorial, be sure and print all nineteen (19) steps displayed over five (5) web pages.** Follow the steps in the Beginner's Tutorial to [download](#), install, and utilize the TrueCrypt encryption software.

- **MAC** - Mac OS X offers native file encryption as well through the use of FileVault. A good step by step guide can be found at <http://www.apple.com/macosx/features/filevault>.
- **Mobile Encryption**
  - **Laptop** - In addition to TrueCrypt, products such as CyberAngel allow for a virtual disk to be created on your hard drive for encryption and require two-factor authentication (two types of passwords in most cases). These products also have

the benefit of having additional features like "call home" where a stolen laptop will broadcast its location if stolen to help in its recovery. You can read more about it at <http://www.thecyberangel.com>.<sup>↗</sup>

- **Phone/PDA** - Downloading e-mail that has sensitive data is a concern.
- **Flash Drives and Recordable Media** (CDs, DVDs, diskettes)- Some flash drives come with their own encryption software as an option. If not, TrueCrypt can be used to create an encryption folder on the drive or recordable media. You will need to install TrueCrypt on your home or personal computer in order to access the encrypted files.