

# Protecting your Data Resources Series - Stop 2

## Tip Sheet – Using Software to Encrypt Data



Disk Encryption software uses a mathematical algorithm to make data unreadable to anyone who does not have the “key” to decrypt it.

There are a number of commercial packages available on the market. Windows Enterprise and Ultimate versions come with BitLocker.

A well known and trusted software is TrueCrypt. It is also an Open Source software, meaning you can get it and use it for free.

You can get TrueCrypt online: <http://www.truecrypt.org/>

### TECHNICAL SUPPORT

Need some help?

Call your regional IT Specialist or the First Call Help Desk.

Steve Paz, Lubbock

Weldon Floyd, Stephenville

Aimee Sandifeer, Overton

Greg Thomas, Bryan

Pete Flores, Corpus Christi

Jeffrey SoRelle, San Angelo

First Call

Toll Free 866 996 2056

College Station 979 985 5737

Looking for more on Security?

Try:

<http://ait.tamu.edu/security.shtml>

<http://ittoolbox.tamu.edu>

Prepared by:

Jim Segers

AgriLife Information Technology

### TrueCrypt Details

You can use three methods to create a storage volume to encrypt sensitive data. You can create a file, called a container, you can encrypt an entire drive, such as USB backup drive, or you can encrypt all your computer's system drives.

Generally for office use you will want to use the File/Container method or encrypt a USB drive or memory stick. Encrypting all your computers drives isn't really necessary.

The best protection for sensitive data is to purchase a specific removable drive for that purpose and to encrypt the entire drive. The protect the removable drive by locking it in a safe place.

TIP: There are USB drives on the market, such as IronKey that do their own encryption.

You can also make the TrueCrypt storage volume hidden if you choose as an added layer of protection. Even if your password key is discovered the volume is not readily visible.

Use the AES 256-bit option, when creating the volume; use the default “hash algorithm.”

If you are creating a container set the size you will need, if you encrypt a whole drive it will use it all.

Enter a password, longer is better. You can also create optional key files for another layer of protection.

Finally format the volume, use either FAT or NTFS file systems, NTFS is the XP, Vista, Windows 7 file system.

Once created, you must run TrueCrypt and “mount” the volume to gain access to the files. So if you use more than one computer, remember to install TrueCrypt on all of them.

There is a beginner's tutorial you should review: <http://www.truecrypt.org/docs/?s=tutorial>

Helpful YouTube video:

<http://www.youtube.com/watch?v=nemmSS5mqDA>