

Title: Data Encryption and Shredding Guidelines**I. PURPOSE**

This guideline helps those who need to put confidential information on their PC local drive, network drive, USB drive, etc. The *Computer and Data Security (8-4)* policy discourages employees from placing confidential information on local drives or mobile devices and when it is necessary requires such data be encrypted. It further recommends such data be securely erased or shredded when no longer needed.

II. WARNING

Once a file has been password encrypted, it cannot be retrieved if the password is lost or forgotten. Depending on how difficult it is to recreate the file or how much cost or inconvenience would be incurred by losing the file, measures should be taken to remember the password. For example, the password could be written down and locked securely away. Likewise, when a file is shredded, it cannot be retrieved.

An encrypted file is only effective if the password is strong, so it cannot be cracked. A strong password contains at least eight characters using at least three of the four character sets (uppercase alpha, lowercase alpha, numeric, and special characters) and is not a word or name.

III. DEFINITIONS

Confidential information is protected by law, policy, or contract and can be disclosed only to those authorized. Examples include social security numbers, credit card numbers, student grades, etc. For practical purposes you may also want to consider as confidential any information that would be embarrassing, upsetting, or inappropriate if improperly disclosed. Examples include salaries, performance reviews, budgets, etc.

Encryption is the process of completely changing data so it can only be retrieved and seen by entering a correct password.

Shredding (also known as securely erasing) a file not only erases pointers to the file, but also writes over the entire file space to make sure the original data cannot be recovered.

IV. ENCRYPTION GUIDELINES

This guideline gives suggestions on how to encrypt information in a variety of situations. The guidelines below generally range from easier to more difficult to implement.

1. Microsoft Word and Excel files can easily be encrypted and password protected by going to *Tools>Options>Security*, entering a password in the “Password to open” field, and clicking on “OK”. This can be done in WordPerfect and QuattroPro by checking the “Password protect” box when saving the document.
2. Those who need to put confidential information on mobile (and easily lost) USB drives can purchase a *Kingston DataTraveler Secure* USB flashdrive, which automatically encrypts anything put on it. Macintosh users should use a *Lexar JumpDrive Secure II Plus* USB drive. These brands may be substituted with others that provide built-in encryption. Encrypted USB drives cost more than

standard USB drives. Option 3 below can also be used to encrypt data on a regular USB drive.

3. Windows (2000, XP, Vista) and Mac OS X (tiger, leopard) users can install an open source, freeware product called TrueCrypt. This will allow them to create and mount an encrypted volume on a local drive, network drive, USB drive, CD, or DVD. Any files created or “dragged and dropped” on the encrypted drive are automatically encrypted. Follow these steps:
 - a. Install TrueCrypt version 5.1.a.
 - b. Read the tutorial and user guide that comes with TrueCrypt.
 - c. Create an encrypted volume on the desired drive (local, USB, CD, etc.)
 - d. Mount the encrypted volume.
 - e. Place files with confidential information on the encrypted drive.
 - f. Make sure all files, including encrypted files, are backed up regularly.

V. SHREDDING GUIDELINES

This guideline gives suggestions on how to securely erase computer files in a variety of situations.

1. If you are erasing a file that is encrypted with a strong password, you do not need to shred it.
2. If there is confidential information on a computer being sent to surplus or elsewhere on campus for re-use, you may request the disk be securely erased by your Technology Support Specialist.
3. Macintosh OS X users can use built-in Disk Utility to shred files.
4. Windows users can install a freeware product called Eraser version 5.7. This will give them the option to select “erase” instead of “delete” in the Explorer window, which will shred the file.