

**TEXAS A&M UNIVERSITY-CORPUS CHRISTI**  
**Sensitive Information Protection Recommendations**

---

### **Locating, Storing, and Removing Sensitive Information**

The following is a list of tools that can be used to secure sensitive information. This list will help individuals locate, store, and remove sensitive information on their systems. As each department and individual may have different requirements, many combinations of the tools will be the norm across the university. The tools listed here are just a starting point. There are many other commercial and free tools available depending on the technical capabilities of the individual protecting sensitive information. Each individual should check with their information technology staff to answer any questions regarding which tools to use and how to use them. Special care should be taken when encrypting sensitive information that is necessary for business purposes. The passwords, passphrases, or encryption keys should be securely maintained so that a manager or other authorized personnel can access the information in the case of a forgotten password or emergency.

Additional guidance and training related to these and other tools will be available through Media and Computer Services as they are developed. Until such time, the IT staff of each department should familiarize themselves with these tools so that they may provide guidance and technical support.

#### **Locating Sensitive Information**

<b>Tool Name</b>	<b>Operating System</b>	<b>Website</b>
Cornell's Spider	Window/Linux/OS X	<a href="http://www.cit.cornell.edu/security/tools/">http://www.cit.cornell.edu/security/tools/</a>

- DO NOT automatically delete files detected by this software.
  - Each file should be examined to determine if it does indeed contain Social Security Numbers and if they are necessary for business purposes.
  - This tool will locate files that do not contain Social Security Numbers. These files should be examined as a precaution.
  - Automatically deleting files could adversely impact the performance and availability of your system.
- DO NOT contact the Cornell support staff with questions about this tool. All questions should be directed to the Faculty/Staff Help Desk or the IT Security Manager.

#### **Secure Storage**

<b>Tool Name</b>	<b>Operating System</b>	<b>Website</b>
WinZip 11.1	Window	Contact the Faculty/Staff Helpdesk
Truecrypt	Windows/Linux	<a href="http://www.truecrypt.org/">http://www.truecrypt.org/</a>
Secure Disk Image	OS X	<a href="http://security.tamucc.edu/osx_encrypted_image.php">http://security.tamucc.edu/osx_encrypted_image.php</a>

- Versions of WinZip older than version 11.1 may not have the capability to encrypt files.
- The university is currently in the process of purchasing enough licenses of WinZip 11.1 to cover university employees. It will not be available until the purchase is complete.

**TEXAS A&M UNIVERSITY-CORPUS CHRISTI**  
**Sensitive Information Protection Recommendations**

---

The projected availability is early August, 2007.

- Strong passwords and passphrases should be used when encrypting sensitive information. See University Procedure 21.01.06.C2.15 Password for guidance.
- Passwords and passphrases that are used to encrypt sensitive information must be protected so that the information can be accessed if the original custodian of the information is unavailable. See the “Password Storage Tools” section for recommendations.

### Secure Delete

Tool Name	Operating System	Website
Eraser	Windows	<a href="http://downloads.sourceforge.net/eraser/eraser582setup.exe?modtime=1167297344&amp;big_mirror=0">http://downloads.sourceforge.net/eraser/eraser582setup.exe?modtime=1167297344&amp;big_mirror=0</a>
Microsoft Remove Hidden Data Tool	Windows Office 2003 and XP	<a href="http://support.microsoft.com/kb/834427">http://support.microsoft.com/kb/834427</a>
Wipe	Linux	<a href="http://wipe.sourceforge.net/">http://wipe.sourceforge.net/</a>
Mac Built-in Secure Delete	OS X	<a href="http://www.apple.com/macosx/features/security/">http://www.apple.com/macosx/features/security/</a>

- Files deleted on Windows and Linux systems are not completely removed until they have been overwritten with new information.
- Information deleted from Microsoft Office documents is maintained as hidden data so that it can be restored if necessary. A special tool is required to remove this hidden data.
- Files deleted on Mac OS X are overwritten automatically and do not require any additional software or user interaction.

### Password Storage Tools

Tool Name	Operating System	Website
Keepass	Windows	<a href="http://keepass.info/">http://keepass.info/</a>
KeepassX	Linux/OS X	<a href="http://keepassx.sourceforge.net/">http://keepassx.sourceforge.net/</a>
Password Safe	Windows	<a href="http://passwordsafe.sourceforge.net">http://passwordsafe.sourceforge.net</a>
Password Gorilla	Windows/Linux/OSX/BSD/Solaris	<a href="http://www.fpx.de/fp/Software/Gorilla/">http://www.fpx.de/fp/Software/Gorilla/</a>