

Sensitive Information

Keeping information safe

Related Tip Sheets: Practice Safe Computing | Keeping High Risk Files Safe

Introduction

Stolen information can result in identity theft and compromise. Unprotected information can be stolen from anywhere at any time. It can be taken when you least expect it. Sensitive information is not limited to just social security numbers or credit card numbers. It also includes student information and grades, human resource data, and private research data, as well as other types of information.

This tip sheet provides information about the safest practices for handling sensitive information.

Accidental Exposure

Sensitive information can become public with a click of the mouse. Take a good look at the way you store and share sensitive information. It is spread everyday through minor human errors that can be easily prevented.

- **Unnecessary records:** Always know what personal information is required to complete any transaction. Never ask for or supply more than is necessary.
- **Taking the easy way out:** Never bypass security protocols for an easier way or an old habit. Future consequences can far outweigh the few seconds you may save.
- **Improper handling:** Everyone capable of accessing sensitive information should be made aware of its importance and be trained in handling it.
- **Forgetfulness:** Be aware of the location of any sensitive information at all times. See Identity Finder below for help with finding sensitive information on your computer.

Safe Practices

Make sure your system for handling sensitive information meets NSIT's suggestions for safe computing:

- **Protect your passwords:** Use good password practices to keep your information safe.
- **Use your computer's firewall:** Make sure that your computer's firewall is turned on.
- **Use the highest safety settings:** Set the safety settings on web applications to the highest level.
- **Remember to log out of web applications:** If you're using a public machine, remember to explicitly log out and quit the browser.
- **Be careful when using wireless networks:** Never use an insecure wireless internet connection when accessing sensitive information over the web.

For more information about safe computing practices, visit nsit.uchicago.edu/safecomputing.

University Policies for Sensitive Information

- **Regulated Computers:**
nsit.uchicago.edu/regulatedcomputers
- **Digital Use of the Social Security Number:**
nsit.uchicago.edu/policies/ssn



Tools for Keeping Information Safe

NSIT offers two free services to help you keep sensitive information safe. For information about storing and sharing Microsoft Office files safely, see our *Keeping High Risk Files Safe* tip sheet.

WebShare

When you need to share a file containing sensitive information, do not send the file via email; instead, place it on WebShare and share a link to the file. Be sure that you give permission only to the person(s) you wish to see the file. Learn more about using WebShare at nsit.uchicago.edu/webshare.

Note: Some departments have established alternative file sharing systems for their staff; check with your department to find out whether such a system is in place for your department.

Identity Finder

Use Identity Finder to search your computer for sensitive information that has been saved there, such as credit card numbers, social security numbers or passwords. This program will help you know if your information is vulnerable to theft. Download Identity Finder at nsit.uchicago.edu/identityfinder.

For additional assistance

Please email support@uchicago.edu or call 4-TECH



THE UNIVERSITY OF CHICAGO
NSIT Networking Services & Information Technologies