

Keeping High Risk Files Safe

Storing and Sharing High Risk Microsoft Office Files Safely

Introduction

High Risk files contain data whose loss or corruption might lead to legal or significant contractual liability, impair the ability of the University to perform its business or academic functions, significantly damage the image or reputation of the University, or otherwise result in legal, financial, or business loss. This data requires tight audit and access controls and should be available only on a "need to know" basis.

High risk data should be encrypted when possible. This tip sheet provides information on storing and sharing high risk Microsoft Office files.

Storing a high risk file

When storing or sharing a high risk file, you should first encrypt the file so that you don't disclose private information in ways that may harm yourself or someone else.

How to encrypt a file

For instructions on how to encrypt a Microsoft Office file, visit <http://nsit.uchicago.edu/docs/encryption>. We will issue a recommendation for encrypting non-Office files in 2009. An encryption key is a common term for an encryption password. Read on to learn how to encrypt your Microsoft Office files. **If you lose your encryption key, your data is gone. DO NOT LOSE IT!**

Important Notes:

Don't use your CNet password as encryption keys for your files. If you need to move a high risk file, encrypt it before moving it. You *must* protect your high risk files through encryption.

Sharing a high risk file safely

Once you've encrypted a file, choose one of the following methods to share a sensitive file:

1. You can share data with a recipient if you are both using the same network drive, such as the Tank file servers. For the data to be accessible both parties must have access to Tank. To request file space on Tank, contact support@uchicago.edu.
2. If the recipient has a CNetID, you can share your file using WebShare's "permissions" feature. You can allow access only to those whom you wish to see the data. For instructions, see <http://nsit.uchicago.edu/docs/webshare/sharing>.
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.
3. If the recipient does not have a CNetID, you can still share your file using WebShare by making a password-secured ticket. For instructions, see <http://nsit.uchicago.edu/docs/webshare/tickets>.
4. You can email an encrypted document to the recipient. However, you should transmit the retrieval key over the phone, by physical mail, or in person.



To learn about the University's policy for computers that contain sensitive data, see the Regulated Computer Policy at <http://nsit.uchicago.edu/technicaltools/regulatedcomputers>.

If these tips don't meet your needs, contact your local support person or NSIT. To see a list of computer support groups, visit <http://nsit.uchicago.edu/unitsupport>.

To learn about other tips for safe computing, visit <http://nsit.uchicago.edu/safecomputing>.

Tip sheets are in progress for the storage and handling of moderate, and low risk files.

For additional assistance

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



THE UNIVERSITY OF CHICAGO
NSIT Networking Services & Information Technologies