IS Data Security Guidelines

These guidelines supplement, not replace, Cornell Policies, non disclosure agreements, etc.

Recommendations for storing confidential data:

- Set screen saver to 15 minutes or less and require password on resume.

- Do not put any confidential university data on any laptop, workstations, hard drive, or removable device that is not encrypted.

- Whenever possible store files containing confidential data on a server secured in the CIT server farm.

- When you complete a project or piece of work and no longer need the confidential data, remove the data as from your encrypted location or the fileserver.

- Do not store confidential university data on any personally own computer.

Understanding the data that is on your computer:

- Execute Identity Finder or Spider at least monthly, review the results, and remove unneeded files.

- Be alert to data you may receive as attachments and remove any confidential data as soon as possible and remind the sender not to send confidential data via email.

- Recognize that some software will copy data to temp files without your knowledge. As you become aware of when and where this occurs, try to clean up these files. When scripts are provided to clean-up these files, it should be executed at least monthly.

Other precautions for securing University data:

- When it is necessary to transfer sensitive data, use a secure transfer method (examples: SFTP, dropbox, etc.) If an outside vendor does not support any secure transfer method we have to work within their limitations, but IS management, functional user area, and security should be aware of these exceptions.

- Use of remote desktop to your machine at work is acceptable if the connection is encrypted. Use of VPN when using remote desktop will enforce encrypted connection. Use fileservers and encrypted containers for data storage when possible.

- If it is necessary to print sensitive information, it should be in your control or in a locked compartment until it can be securely shredded.

- When using tools to access sensitive data, do not select the 'remember me' or 'save password' options. If your computer is stolen, this could expose entire databases or applications. Terms:

Confidential refers to data classified by the university as needing the highest level of protection. Confidential data is subject to more stringent security requirements than other university data. The following data elements, when they appear in conjunction with an individual's name or other identifier, are classified as confidential:

- Social Security numbers
- Drivers license numbers
- Credit card numbers
- Bank account numbers
- Patient treatment information

Sensitive data refers to data that may not be classified as confidential but should be protected as well. This includes data such as salary information, home address, data on university gifts.

Familiarize yourself with information and policies below:

Protecting University data:http://www.cit.cornell.edu/security/data/index.cfm

Review Security of Electronic University Administrative Information: http://www.dfa.cornell.edu/dfa/cms/treasurer/policyoffice/policies/volumes/informationtech/upload/vol5_10.pdf

Use of university owned computer equipment - see: http://internal.cit.cornell.edu/Internal_Computer_Policies/Univ_Owned_Equip.html

Voyeurism - refer to Data Stewareship & Custodianship Policy -- http://www.dfa.cornell.edu/dfa/cms/treasurer/policyoffice/policies/volumes/governance/upload/vol4_12.pdf   especially the section "**General Prohibitions".** Note: data modifications you do in non production environments to accomplish your job are fine. Data modifications to production that are requested by the appropriate user office and tracked according to IS policies are fine.