CEHS Policy on Securing Sensitive Data
April 2014

Recent news reports provide numerous examples of hackers gaining access to sensitive information. These reports highlight the extreme difficulty in securing digital information and the serious consequences when a breach does occur. As a college and as individuals we have an obligation to do all we can to protect the privacy of individuals whose data we manage. Failure to protect sensitive data has serious and costly consequences for our constituents, for the college, and for faculty and staff.

Sensitive Information
Sensitive information includes personally identifiable information such as social security numbers, credit card numbers, driver's license numbers, or other personal information that might contribute to identify theft. Files that contain information about students, research subjects or clients are also critical.

We have obligations to protect against the inappropriate release of personally identifiable information under:

- **University policy** (http://its.unl.edu/ssn)
- **Nebraska law** (http://uniweb.legislature.ne.gov/laws/statutes.php?statute=s8708002000)
- **Family Education Rights and Privacy Act** (FERPA)
- **Health Insurance Portability and Accountability Act** (HIPAA)
- **Institutional Review Board policies**

If you are storing sensitive information, you must report this to the University by filing a report through the Personal Identity Information Inventory Tool found at http://its.unl.edu/ssn.

Eliminating Sensitive Information
The only effective way to eliminate risk is to remove sensitive information from computers and mobile devices. We often maintain email, advising records, grade rosters, research data, and other files when they are not necessary. Deleting these files is critical. When we do need to legitimately keep files we must eliminate the sensitive information from those files.

Identifying the location of sensitive information can be very difficult, particularly when we have email or archived files that we may have not looked at for some time.

Identify Finder is a program UNL provides to scan computers and assist in locating these files. CEHS Tech Support is in the process of installing and running *Identify Finder* on all CEHS faculty and staff computers. If you do not run *Identity Finder* on your computer(s), you should develop and document an alternate method of verifying that sensitive information is not being stored on your computer.

Security Best Practices
You should also protect yourself and your data by observing security best practices, including the following:

- **Protect your password**. Use strong passwords and do not share or use the same passwords on multiple sites. For more information see http://its.unl.edu/creating-curiously-strong-passwords. There are a number of available software applications that make the process of generating and managing multiple passwords easier and more efficient.
- **Keep your operating system and software up to date**. When updates become available install them as soon as possible. CEHS Tech support has client management tools to help assist with this. For more information see http://its.unl.edu/desktop/client-management-tools.
- **Use UNL Virtual Private Network (VPN)**. When you are off campus use the UNL VPN to access resources on campus. This allows for encrypted communication between your computer and computers on campus. For more information see http://its.unl.edu/vpn.
- **Encrypt files on your computer**. You may encrypt all or a portion of the files on your computer. This may be particularly important on laptops.
- **Install and run current antivirus software**. CEHS IT Support installs antivirus software on all CEHS computers. For your home computer(s), you can download software from http://antivirus.unl.edu/unl-antivirus.

For more information
It is your responsibility to be aware of the types of data you store and to protect it. You can learn more from the following two sites.

- **UNL Data security guidelines and the definitions of data types** (http://go.unl.edu/data-class)
- **Security and best practices** (http://security.unl.edu)

CEHS IT Support
CEHS IT Support staff can provide help in making your computers and devices more secure. For assistance, please submit a help ticket @ http://cehshelp.unl.edu or call 2-0096 and a ticket will be created for you.