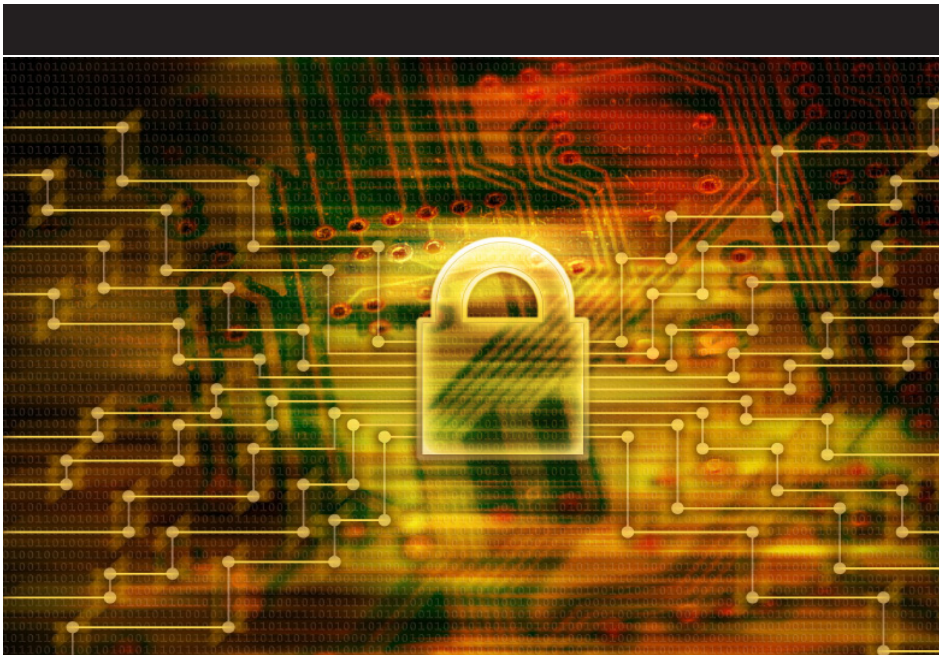
The Ohio State University at Mansfield
Office of Information Technology
Ovalwood Hall
Mansfield, Ohio 44906
419-755-4220



Best Practices for

Sensitive Information

All Ohio State Mansfield Informational Technology (IT) equipment and information resources remain the property of The Ohio State University and not of particular individuals, teams or departments. Adhering to "Computing Best Practices" will help ensure Ohio State Mansfield IT resources are used legally and securely. The Ohio State University is very committed to protecting university network resources and restricted data (Social Security Numbers, grades, personally identifying student information, financial data, credit card information, etc.). The expectation is that anyone given sensitive information has the responsibility to securely protect the data. All Ohio State Mansfield computers will have their "My Documents" folder or a "Secure Doc" folder within the "My Documents" folder encrypted for the storage of sensitive data. Macintosh computers use whole disk encryption so sensitive data can be stored in your "User/Docs" folder.

LINKS

Information Technology at OSU

Buckeye Secure: Encrypting Stored Data

Buckeye Secure: Restricted Data Elements

Buckeye Secure: Minimum Computer Security Standard

Locking It Down: Simple Laptop Security

Electronic Files

Password-protect sensitive files. Choose a unique password and avoid easily identifiable information, such as mother's maiden name, birth date, phone number or a series of consecutive numbers.

Use encryption especially when transmitting files with personal information and when storing files on CD, DVD, or portable devices. Windows users can encrypt files and folders with Microsoft's Encrypting File System (EFS). Mac File Vault allows built-in encryption of folders in Mac OS X or higher.

Keep sensitive files in a secure location with limited access and away from non-sensitive files. Identify who requires access to the electronic files and how the information is distributed.

Delete files from all locations (hard drive and network) when no longer valid. Do not hold onto old queries or reports that contain SSN or other personal information. Be sure to wipe files from network and hard drives. Empty your computer's recycle bin and clear temporary file folders.

Avoid using SSN as an identifier. Ask: Is there another way of identifying a user? Is SSN needed in the file?

Avoid emailing sensitive files. If email is necessary, use encryption and password protection. Do not email the password.

Always work with your unit's IT professionals when implementing new technologies. These individuals can help assist with the identification of appropriate tools and methods. Use Technology Services as a resource.

Computers

Install a firewall on your network. Work with Technology Services when considering network or computer firewalls.

Keep software updated; use anti-virus, anti-spam, and anti-spyware software. Use the computer operating system's automatic update functions to check for software updates. Free anti-virus, anti-spam, and anti-spyware are available for university members. Update these as well.

Use password protected screen savers. Use a password protected screen saver to block unwanted views to personal information. Do not leave the password in a visible location.

Manage access to sensitive information. Use authentication to manage access to sensitive information.

Delete all sensitive files and personal information before discarding a computer. The hard drive can also be destroyed in order to prevent any chance of identity theft.

Limit access and never share passwords. Logins should be password protected. Always log out when leaving a computer station (classroom podium computers).

Never use the "remember my password" function. Also change passwords frequently and avoid using easily identifiable information for a password.

Portable Storage Drives

Avoid storing personal information on portable storage devices, such as thumb drives, CDs, DVDs, laptops, PDA, mobile phones, Blackberries, etc.

Protect sensitive information through encryption and password protection.

Do not leave in open or unlocked areas, such as your home, car, or workplace (office). Mobile devices containing personal information should never be left in public places or locations susceptible to theft, such as your car or home.

Use locked laptop stations to prevent theft. These are available through most laptop retailers and can offer secure options for your laptop.

Wipe portable devices clean before discarding or giving to others. Be sure to erase all sensitive information on devices before discarding. Shredding options are available for CDs and DVDs. Mobile phones can store personal data in their memory - be sure to remove this before recycling.