

Basic Data Security Guidelines

Introduction

Your data are a valuable asset, vital to the success of the University's research mission and therefore thoughtful stewardship is required. The security of your data depends on proper computer management and appropriate data handling procedures. The level of required protection depends on several factors including the sensitivity of the data and whether statutory or regulatory requirements exist. In some cases, measures beyond those described here may be required. This document provides the minimum steps necessary to help ensure the security of your computing environment and the information stored within. The Information Technology Center (ITC) Help Desk or your local IT support specialist can provide assistance and answer any questions related to these guidelines.

General Guidelines

- Keep your desktops, laptops, and servers up to date with the latest operating system and security patches
- Keep your applications up to date with the latest vendor supplied updates.
- Run current anti-virus software on all desktops and laptops. MSU provides McAfee Anti-Virus for department use at no charge.
- Run current anti-spyware software. Several free versions are available including Microsoft's Defender, and Spybot Search and Destroy.
- All desktops, laptops, and servers should run a properly configured firewall.
- Maintain the physical security of all desktops, laptops, and servers. This includes locking unattended offices and restricting access to machine rooms.
- Select strong passwords and change them periodically. Passwords should have a minimum of 8 characters and a mix of upper and lower case, numbers, and special characters. Do not use dictionary words or other personal attributes (date of birth, phone number, etc.) Do not share passwords and do not document passwords.
- Eliminate the use of forms that ask for sensitive personal information whenever possible.
- Password-protect all sensitive personal information and accounts with access to sensitive personal information.
- Lock your computer with a password protected screensaver when unattended. On Windows systems, ctrl-alt-del, return or Windows-L will lock your screen.
- Notify ITC or the Enterprise Security Manager if you suspect sensitive personal information may have been exposed.

Storage and Sharing

- Do not store sensitive or critical data on desktop or laptop machines. Instead, use properly managed servers.
- Maintain automated backups to removable media and perform periodic test restores. Store backup media in a secure, separate location.
- Do not transmit sensitive information via laptop, PDA, or any other unsecured wireless technology.

- Do not transmit sensitive information via e-mail or the Internet unless the connection is secure or the information is encrypted.
- Do not store sensitive information on laptop/desktop computers, PDAs, USB drive, CD, flash memory card, or other removable storage media unless used for securely managed routine backups.
- Do not take items containing sensitive information home.
- Do not publicly display sensitive personal information or leave sensitive personal information unattended or unsecured.
- Do not communicate or share confidential student data or other personally identifiable information unless specifically allowed or required by University or regulatory requirements.

Disposal

- Discard media (such as disks, tapes, hard drives, or other removable storage devices) that contain sensitive personal information in a manner that protects the confidentiality of the information.
- Computing systems that are moved or repurposed must have the information on their storage devices properly wiped.
- Shred sensitive personal information when it is no longer needed. Do not discard printed sensitive personal information in the trash.

Relevant Links

Site Description	URL
MSU IT Security	http://www.montana.edu/itsecurity
Board of Regents IT Policies	http://www.montana.edu/wohelp/borpol/bor1300/bor1300.htm
MSU Computing Policies Manual	http://www2.montana.edu/policy/computing_manual/
MSU Policy 400.00 - Acceptable Use	http://www2.montana.edu/policy/computing_manual/comp400.html
MSU Policy 600.00 - Safeguarding Customer Information	http://www2.montana.edu/policy/business_manual/bus600.html
Campus Networking Policy	http://www2.montana.edu/policy/itc/Campus_Networking_Policy.htm
Standards for Network Connectivity	http://www.montana.edu/itac/campusnetstds.doc