Examples of Data Security Best Practices

General Practices

- Password issues
  - Keep passwords strictly confidential. Do not share them with others.
  - Change passwords frequently: every 30 to 60 days.
  - Create passwords containing both numbers and letters and using upper and lower case (e.g., t6UG88).
  - Do not use passwords identifying a personal fact about yourself (e.g., birthdate, child's name).
  - Learn your password. If you must write it down, keep the information stored somewhere private and secure.
- Physical security
  - Make it possible to lock desks, offices, and filing cabinets.
  - Emphasize the importance of physical security practices in all data training.
- Send personally identifiable information from education records by email only after using an encryption program or some other means of protecting the integrity of the information.
- Put confidential information into a locked cabinet or drawer when leaving the area where it is in use.
- Have an acceptable-use policy in place regarding both Internet access and confidential data files and establish a procedure for monitoring use.
- Hold all conversations regarding confidential information in nonpublic areas.
- Do not allow confidential data to be worked on at home.
- Institute confidentiality agreements with vendors, employees, and service providers.
- Include acknowledgement of security processes in all appropriate job descriptions.
- Develop and disseminate written security practices.
- Provide ongoing training regarding confidentiality issues and the sensitivity of data.
- When recycling computers, pull or reformat hard drives.

Technical Practices

- Implement an authentication system for logging on to computers and into computer networks. Include an automated prompt to change passwords frequently.
- Set reasonable timeout intervals on computers (5 to 15 minutes), so that after the specified interval of inactivity, the machine will log off the network and its screen will lock, requiring a password to re-access.
- Make sure that wireless networks are secure.
- Implement an appropriate backup system.
- Establish an audit-trail mechanism for identifying users who enter or change critical data.
- Update anti-virus and anti-spyware software frequently.
- Establish plans for reacting to data security breaches.
- When deleting confidential materials, use overwriting software to be sure data are completely deleted.