


Career and Technical Education Information System (CTEIS)
Data Security Do's and Don'ts

- DO change your log-in password frequently.
- DO use password-protected screen savers on computers that store or provide access to sensitive data.
- DO consult your district or ISD Information Technology department on how to keep sensitive data secure and follow their recommendations.
- DO follow all district policies on data security.
- DO identify education record files and data elements within the files as restricted (confidential) or unrestricted.
- DO always look for the Secure Socket Layer (SSL) symbol  (a lock) in the lower right corner of your screen when accessing any secure website, including CTEIS.
- DO use WinZip's encryption feature to encrypt files with sensitive data prior to sending via email or transporting.
- DO always log out/sign off CTEIS when you are finished working or will be stepping away from your computer.
- DO ensure that your computer hard drive is properly "scrubbed" or destroyed if it is to be sold or disposed of. Ensure that decision makers are aware that your hard drive has been used to store sensitive data since "deleted" files are recoverable, even if the hard drive is re-formatted afterwards.
- DO restrict access to sensitive data to only those who need it and are authorized to use it.
- DO maintain anti-virus software on your network and wireless computer and keep it up to date.
- DO know state and federal laws regarding protection of student and employee data.
- DO ensure that data are destroyed according to your agency's records retention and disposal policy and that appropriate disposal methods are utilized.
- DO ensure that people involved in using, coding, entering, and processing confidential information have the necessary training and background to perform their tasks accurately and maintain strict confidentiality and that they understand the criteria, context, penalties, and other considerations.
- DO physically secure paper as well as electronic records by locking up file cabinets, laptop computers, and removable media including portable drives and disks/diskettes.
- DO immediately report any suspected breach of data security to district authorities.
- **DON'T share your password with anyone for any reason.**
- DON'T send sensitive data in the body of an email or as an unencrypted attachment.
- DON'T access CTEIS or any other web-based system with sensitive data using a public computer (such as at a hotel, coffee shop or internet café). There are programs that can record all of your key-strokes and steal your password and later use it to obtain access to confidential data.
- DON'T access CTEIS or any other web-based system with sensitive data using a personal computer on an unsecured wireless network.
- DON'T retain data beyond its useful life.
- DON'T transport secure data on a Thumb drive. If you must, ensure that the thumb drive is encrypted
- DON'T write your password down, and if you must, it should be in a secured location
- DON'T allow Windows to 'remember the password' if you are using a public computer,

References and Resources

National Forum on Education Statistics. *Forum guide to protecting the privacy of student information: State and local education agencies, NCES 2004-330*. Washington DC: 2004.

National Institute of Standards and Technology. *Users guide to securing external devices for telework and Remote Access: Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-114*. Gaithersburg, MD: 2007.

<http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf>

State of Michigan cyber security website: <http://www.michigan.gov/cybersecurity>. Includes a quiz to test your knowledge.

Secure Florida website. Has a great deal of useful information on keeping data secure:

<http://www.secureflorida.org/>