

## Data Handling Best Practices

The University of Northern Colorado is responsible for the confidentiality and integrity of their data under existing federal, state and local legislation. This document is written to convey some “best practices” when handling and managing University sensitive, confidential or private data.

Personal Identifiable Information (PII) that can be used to steal identities, disrupt University operations and damage UNC’s reputation includes:

- a) Social Security Numbers (SSNs)
- b) Health Information – including immunization information, FMLA information and
- c) Credit Card information
- d) Non public directory information – including student grades

The following recommendations have been compiled to assist you in keeping University PII data secure. *REMEMBER: It is important to treat other people’s information as if it was your own.*

While not a good idea, it is often necessary to save PII data either on your desktop/laptop computer or the network. Laptops containing PII data MUST use either Utimaco for Windows or File Vault for Macintosh and the PII data must be saved in an encrypted folder/directory. If you must save your data to the network, it should be saved in your home directory (h:drive).

In all cases, please follow these simple rules.

- ◆ Assign a complex passphrase as your personal digital identifier (PDID)/login;
- ◆ Don’t use Internet files sharing software such as Kazaa or BitTorrent.;
- ◆ Do not remove or alter your computer’s antivirus and firewall application settings;
- ◆ Delete files from ALL locations (hard drive and network drive) when no longer valid. Do not hold on to old queries or reports that contain personal information. Empty your computer’s recycle bin and clear temporary file folders
- ◆ Shut down or turn off the computer when not in use;
- ◆ Never share passwords;
- ◆ Avoid emailing sensitive files. If email is absolutely necessary, use Windows Rights Management encryption. (see WRM information below);
- ◆ Use a password protected screen saver;



- ◆ Always use encryption when transmitting (emailing) or saving files on CDs, DVDs, PCs, Macs, portable devices, etc. that contain personally identifiable information;
  - Windows users
    - encrypt files and folders with:
      - Utimaco—encryption software for Windows XP/2000/2003. Encryption is automatic, real-time (on-the-fly) and transparent.
    - OR
      - Microsoft’s Windows Rights Manager (WRM) – A Microsoft technology used to encrypt confidential documentation. Specific functions such as printing, copying, editing, forwarding, and deleting can be applied by the creator of any piece of information. NOTICE: Macintosh users cannot decrypt WRM files or email messages and an *alternative campus standard solution will be forthcoming*.
  - Macintosh users
    - encrypt files and folders with
      - File Vault- Apple's OS X built-in, secure encryption technology for a user's files and folders. FileVault encrypts a user's entire directory, settings and all data.
      - Microsoft’s Windows Rights Manager (WRM) will **not** function on a Macintosh. If you receive a file or directory that has been WRM'd you will not be able to decrypt it. *An alternative campus standard solution will be forthcoming*.
  - Linux Users
    - Truecrypt
      - TrueCrypt is a software solution that allows for secure storage of data. No data stored on an encrypted volume can be read without using the correct password.

**PRINTING:**

- Printed reports with PII data must contain the creator’s name, date and time, data source (OBIA, Data warehouse, IT, etc.) and a confidential notice.
- Limit display of personal information. Do not leave paper containing personal information on desks or in open view; avoid printing SSN unless required by law.
- Always store paper reports containing PII in a secure location such as a locked filing cabinet and know who has access to the location. Avoid taking PII reports with you to unsecured locations such as your home or car.
- Shred paper with PII before discarding.
- Limit distribution of documents with PII and know who is receiving the documents and how it will be used.

For additional information on protecting your data please visit [www.unco.edu/cybersecurity](http://www.unco.edu/cybersecurity) or email [security@unco.edu](mailto:security@unco.edu)