



Sensitive and Protected Data Management Procedure

Revision History

Version	Date	Editor	Nature of Change
1.0	11/14/06	Kelly Matt	Initial Release

Table of Contents

1.0 Overview.....	1
2.0 Purpose.....	1
3.0 Scope.....	1
4.0 Protected Data.....	1
5.0 Hard Copy Data	1
5.1 Storage	1
5.2 Transport.....	1
6.0 Electronic Data.....	1
6.1 Storage	1
6.2 Transport.....	2
7.0 Disposal.....	2
7.1 Physical.....	2
7.2 Digital	2
8.0 Enforcement.....	2
9.0 Related Policies, Procedures, and Codes of Conduct.	2

1.0 Overview

All individuals who access the University of Northern Colorado's computing infrastructure have a responsibility to safeguard data. This procedure establishes the rules by which protected data should be managed and used within the University.

2.0 Purpose

This document aids in establishing clear guidelines for managing protected data.

3.0 Scope

This Procedure applies to employees, contractors, consultants, temporary employees, and other workers at UNC including all personnel affiliated with third parties.

4.0 Protected Data

All Personally Identifiable Data (PII) which includes but is not limited to any data protected under a federal or state statute is considered protected data. This includes but is not limited to Family Educational Rights and Privacy Act (FERPA) protected data and Colorado HB 03-1175 protected data. In addition credit card numbers, expiration dates, and Card Verification Value (CVV) are also considered protected data.

5.0 Hard Copy Data

Hard Copy data is defined as data that is not stored in electronic form. This includes printed material in any form. Reports, Rosters, Extracts. This also includes credit card receipts and carbons

5.1 Storage

Protected data in hard copy format, when not attended or in used should be stored in a secure location such as a locked drawer or file cabinet. Do not leave protected data in out in the open for example on desk or printers.

5.2 Transport

When transporting protected data make sure that the data is obscured from plain sight. Use sealed envelopes for both external and interoffice mail when protected data is involved.

6.0 Electronic Data

Electronic data is data that is stored in electronic format, regardless of storage media. This includes but is not limited to the following:

- Network Drives
- Local hard Drives
- Laptops
- PDA
- Thumb drives

Regardless of where the data exists the following guidelines should be followed for all protected data.

6.1 Storage

Protected data should be stored on secure UNC IT managed devices only. Protected electronic data should not be transferred to an individual's personal computing equipment or to a non-approved third party. Protected data that exists outside approved systems such as Banner must be stored using the UNC approved document management system, Window Rights Management (WRM).

Efforts should be taken to protect data in approved data stores such as encrypting various fields to limit the usefulness of data if systems are compromised.

6.2 Transport

When protected data is transported electronically UNC IT approved encryption methods should be used. At present this includes Secure Sockets Layer (SSL) encryption and WRM. SSL is commonly used in web applications and WRM can be used to encrypt Microsoft office files and email. Do not transport any protected data within or outside the university with out utilizing one of these encryption technologies. This includes email, FTP or any other method of electronic transport.

7.0 Disposal

Media disposition is a key element in assuring data confidentiality. Confidentiality is the ability to restrict access to information based on the value of the information. This includes protecting personally identifiable information.

In order to provide appropriate controls on the information we are responsible for safeguarding, we must properly safeguard media in all forms.

7.1 Physical

When disposing of protected data in physical hard copy format please ensure that you are adhering to the following guidelines:

- Place all protected in the appropriate locked and protected bin.
- Do not stuff or over fill bins.
- If bins are not available or data is highly sensitive cross-cut shred immediately

7.2 Digital

When disposing of protected data in electronic format please ensure that you are adhering to the following guidelines:

- Purge, degauss, shred, or physically destroy electronic media so that protected data cannot be reconstructed.

To facilitate secure disposition of electronic media UNC Information Technology provides a secure drop service in the basement of Carter Hall at the operator's window. Individuals can bring digital media to this area and for secure disposal.

For more detailed information on appropriate information and media disposition please see the [Media Disposition and Sanitation Procedure](#).

8.0 Enforcement

Any person found in violation of Federal, State law or University policy, regulation or procedures is subject to loss of privileges, disciplinary action, personal liability and /or criminal prosecution. The University may block access to or remove a network connection that is endangering computing and or network resources or that is being used for inappropriate or illegal use. Information Technology will work with the Dean of Students, the UNC Police the academic deans and directors and others to enforce this policy.

9.0 Related Policies, Procedures, and Codes of Conduct.

All applicable laws and University policies, regulations and procedures bind UNC students and employees.

- UNC Acceptable User Regulation:
- Media Disposition and Sanitation Procedure: