

Effective Date: 8/1/2005

NORTH CAROLINA CENTRAL UNIVERSITY



1801 Fayetteville Street  
Durham, NC 27707

### Information Technology Services

New School of  
Education  
712 Cecil Street, 3rd.  
Floor  
Durham, NC 27707  
(919)-530-7676

[www.nccu.edu/helpdesk](http://www.nccu.edu/helpdesk)

Updated: August 2005

# Data and Information Policy

Supersedes Policy Dated: New Policy

Approved: by the NCCU Board of Trustees on February 15, 2006

## Purpose of Policy:

The expansion of computerized applications at North Carolina Central University has created an environment where there is wider access to systems and to sensitive databases and information.

The purpose of this Policy is to provide general guidance on the protection of University data and information being processed by manual as well as automated systems and the protection of the records and reports generated by these information processing systems.

## Policy:

Information is a vital component of University operations, and it is important to ensure that persons with a need for information have ready access to that information. It is equally important to ensure that measures have been taken to protect sensitive information against accidental or unauthorized access, modifications, disclosures, or destruction, in order to ensure the security, reliability, integrity, and availability of information. In addition, federal and state laws assign legal responsibility for the correct and appropriate use of information in order to protect a person's right to privacy.

This policy sets forth the responsibilities for data and information security for all individuals and departments at North Carolina Central University who access, process, or have custody of university data.

## Guidelines:

- A. The vice chancellors shall ensure that the standards for data security that affect their respective areas of responsibility are effectively implemented. The administrative duties associated with this responsibility shall be assigned by the vice chancellors to the owners of the data, who typically are the managers responsible for either the creation or collection of that data and/or the primary user of that information.
- B. **Owners** of data are responsible for making decisions about the use and protection of information in their custody. Areas of concern shall include:
  1. Accuracy and completeness of data and information;
  2. Classification of data as confidential (subject to privacy laws), sensitive (non-public salary information) or public;
  3. The authorization process to permit access to the information and to terminate access when necessary;
  4. The identification and minimization of risks and exposures;
  5. The utilization of established procedures designed to protect information from unauthorized access or disclosure, whether accidental or intentional;

6. Communication of information protection procedures to authorized users;
7. Physical access to hard copy records, computer terminals and personal computers;
8. Providing procedural safeguards including backing up information for business continuity purposes; and
9. Evaluating security control procedures related to information in their custody.

C. The **users** of information include all persons who have been authorized to read, write or update the information. The users of information have the responsibility to:

1. Use the information only for the purpose that was authorized by the owner.
2. Comply with all controls established by the owner and those delegated by the owner to administer control procedures.
3. Avoid disclosure of confidential or sensitive information to unauthorized persons without the permission of the owner or vice chancellor.
4. Comply with the *Family Educational Rights and Privacy Act* of 1974 and the North Carolina Central University Privacy Policy.
5. Have a signed Confidentiality Statement on file with ITS Planning and Programs.

**Violations:**

The vice chancellors shall be responsible for ensuring that appropriate data and information security procedures are published and distributed to all *owners* and *users* of university information (as defined above). This Policy and all supporting procedures and guidelines distributed pursuant to it shall serve as the standards of information and data security to be applied by owners and users and will be the basis for compliance monitoring, review, and audit.