FAYETTEVILLE STATE UNIVERSITY

Data Classification Policy

Authority:	Information Technology and Telecommunication Services
Category:	University-wide
Applies to:	Faculty and Staff
History:	Approved on … First Issued on January 17, 2002
Related Policies:	Acceptable Use Policy Copyright Ownership and Use Policy - [1.20] Information Security Policy University Email Policy Network Use Policy
Contact for Info:	Chief Information Officer – (672-1477)

I. Purpose

FSU enterprise-level administrative data are an asset owned by the Fayetteville State University (hereinafter "University") and must be protected accordingly. A data policy is necessary to provide a framework for securing data from risks including, but not limited to, unauthorized destruction, modification, disclosure, access, use, and removal. This policy outlines measures and responsibilities required for securing data resources. It shall be carried out in conformity with state and federal law.

This policy serves as a foundation for the University's information security policies, and is consistent with the University's data management and records management standards. The University recognizes that the value of its data resources lies in their appropriate and widespread use. It is not the purpose of this policy to create unnecessary restrictions to data access or use for those individuals who use the data in support of University business or academic pursuits.

II. Scope

This policy applies to all centrally managed University enterprise-level administrative data and to all user-developed data sets and systems that may access these data, regardless of the environment where the data reside (including mainframe systems, servers, personal computers, mini-computers, etc.). The policy applies regardless of the media on which

data reside (including electronic, microfiche, printouts, CD, etc.) or the form they may take (text, graphics, video, voice, etc.).

III. Policy

Data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with data value, sensitivity, and risk.

1. To implement security at the appropriate level, establish guidelines for legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data, data will be classified into one of the following categories:

   Restricted – data whose disclosure to unauthorized persons would be a violation of federal or state laws or University contracts.

   Public – data to which the general public may be granted access in accordance with the North Carolina Public Records Act.

   Data in both categories will require varying security measures appropriate to the degree to which the loss or corruption of the data would impair the business or research functions of the University, result in financial loss, or violate law, policy or University contracts.

   Security measures for data are set by the data custodian, working in cooperation with the data stewards, as defined below.

2. The following roles and responsibilities are established for carrying out data policy:

   Data Trustee: Data trustees are senior University officials (or their designees) who have planning and policy-level responsibility for data within their functional areas and management responsibilities for defined segments of institutional data. Responsibilities include assigning data stewards, participating in establishing policies, and promoting data resource management for the good of the entire University.

   Data Steward: Data stewards are University officials having direct operational level responsibility for information management – usually department directors. Data stewards are responsible for data access and policy implementation issues.

   Data Custodian: Information Technology Services is the data custodian. The custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by data trustees or their designees (usually the data stewards), and implementing and administering controls over the information.

   Data User: Data users are individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a

position of special trust and as such are responsible for protecting the security and integrity of those data.

3. Clarification of roles in data classification is the responsibility of the Banner Data Standards Committee and the Management of the Information Technology Services Division.

4. Enforcement

   Enforcement measures implemented for data security will be dictated by the data-classification level. Measures will include an appropriate combination of the following:

   a. Encryption requirements
   b. Data protection and access control
   c. Documented backup and recovery procedures
   d. Change control and process review
   e. Data-retention requirements
   f. Data disposal
   g. Audit controls
   h. Storage locations
   i. User awareness

5. Review

   The Chancellor has approved the Data Classification Policy. The Chief Information Officer will review the policy periodically and bring concerns to the Information Security Committee, which will recommend revisions as appropriate.

6. Links to Related University Policies

   Acceptable Use of Computing Policy
   Information Security Policy