ELIZABETH CITY STATE UNIVERSITY
Data Classification Policy

Preamble

Data stored here at Elizabeth City State University is a critical asset. All employees of the University community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form). Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of data belonging to the University to be in compliance consist 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.

1. 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.).

2. 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.

   A. 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:

      i. Restricted – data whose disclosure to unauthorized persons would be a violation of federal or state laws or University contracts Examples include student or employee identifiable information. (i.e., Social Security Number, birth date, driver’s license number, etc.), financial records, medical records, legal records, student records, police records, and credit
card information. Unauthorized disclosure of restricted information could result in adverse legal, financial or reputational impact upon the University).

ii. **Public** – data to which the general public may be granted access in accordance with the North Carolina Public Records Act. (Examples include public web pages, course listings, press releases, marketing brochures, etc. While the requirements for protection of public data are less than that of Restricted and Sensitive, sufficient controls must be maintained to protect unauthorized modification of data).

iii. **Sensitive** – sensitive data is information that business units may decide to share with other units outside their administrative control for the purpose of collaboration. This information is not information that meets the requirements of “non-public” information. (Examples include data created by the department, research data, and project data. Loss of this information could cause harm to the University’s image or reputation, but would not necessarily violate existing laws or regulations).

Data in all 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.

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

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

i. **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.

ii. **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.

iii. **Data Custodian**: Information Technology 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.

iv. **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.

Clarification of roles in data classification is the responsibility of Administrative Computing department of the Information Technology Division.

3. **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. Banner Security Policy
B. Acceptable Use of Technology for University Employees
C. Network Security Policy

4. **Review**

The Director of Administrative Computing will review the policy periodically and bring concerns to the Chief Information Officer, which will recommend revisions as appropriate.