

DATA CLASSIFICATION POLICY**1. Purpose**

BCC enterprise-level administrative data are an asset owned by the Brunswick Community College at Supply (hereinafter "College") 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 College's information security policies, and is consistent with the College's data management and records management standards. The College 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 College business or academic pursuits.

2. Scope

This policy applies to all centrally managed College enterprise-level administrative data (Datatel's Colleague using UniData database running on a Unix operating system) 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.).

3. 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:

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

2. 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 College, result in financial loss, or violate law, policy or College 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:

1. Data Owner: Data Owners are senior College 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. Examples of these include UT, ST, CF, and HR. Responsibilities include assigning data stewards, participating in establishing policies, and promoting data resource management benefitting the entire College.

2. Data Steward: Data stewards are College officials having direct operational-level responsibility for information management – usually department directors. Data stewards are responsible for data access and policy implementation issues. Data stewards and data owners may act in both roles as one responsibility.

C. **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 Owners or their designees (usually the data stewards), and implementing and administering controls over the information.

D. **Data User:** Data users are individuals who need and use College data as part of their assigned duties or in fulfillment of assigned roles or functions within the College 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.

E. **Data Accessibility:** Access is provided to an employee by Information Technology staff upon receipt of a completed authorized CARF (computer access request form) and a signed copy of the College's confidentiality agreement.

Clarification of roles in data classification is the responsibility of the Information Technology Services department.

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:

- 1) Encryption requirements
- 2) Data protection and access control
- 3) Documented backup and recovery procedures
- 4) Change control and process review
- 5) Data-retention requirements
- 6) Data disposal
- 7) Audit controls
- 8) Storage locations
- 9) User awareness

5. Review

The Director of Information Technology Services has submitted the *Data Classification Policy* pending Board of Trustee approval. The Director of Information Technology Services will review the policy periodically and recommend revisions as appropriate.

6. Links to Related College Policies

[Enterprise Systems Policy](#)

[Acceptable Use of Computing and Electronics Resources Policy](#)

[Security of Networks and Networked Data Policy](#)

Approved by Brunswick Community College Board of Directors
June 9, 2010; June 28, 2013; February 19, 2018