Title: Data Classification Policy

- □ Initial Action: 11-28-18
- □ Board Resolution: 18-065
- □ Last Revised
  - □ Policy:
  - □ Procedure:
- □ Last Reviewed:
- □ Effective: 12/6/18
- □ Next Review:
- □ Responsibility: Information Technology

Policy:

This policy serves as a foundation for the College's information security policies. College administrative data are an asset owned by Cecil College (hereinafter "College") and must be managed accordingly. A data policy is necessary to provide a framework for securing sensitive 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.

It is not the purpose of this policy to create unnecessary restrictions to data access or use for those who use the data in support of necessary College functions.

Procedure:

This policy applies to all College data and to all user-developed data sets and systems that may access these data, regardless of the environment where the data resides (including cloud systems, servers, personal computers, mobile devices, 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.).

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 sensitivity and risk.

I. 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 and will be stored in means appropriate to that level of confidentiality:

   A. “Class A” - High Risk: Data with a known protection standard whose release to an unauthorized person would be a violation of Federal or State laws, would potentially result in criminal penalties and requires disclosure to affected parties. Some examples include SSN data, data covered by Health Insurance Portability and Accountability Act (HIPAA), The Federal Information Security Management Act (FISMA), and data covered by Payment Card Industry (PCI) compliance requirements.

B. "Class B" - Moderate Risk: Data not covered by one of the known protection or disclosure standards listed in section A above whose loss, corruption, or unauthorized disclosure would constitute a violation of Federal or State laws, and would potentially result in civil penalties. Some examples include certain types of grant-funded research data, data deemed confidential in contract agreements, Family Educational Rights and Privacy Act (FERPA) data, and some Jenzabar data (excluding SSN and other data as designated in 'A' above).

C. "Class C" - Low Risk: Data not designed for public dissemination, but not falling in the "High Risk" or "Moderate Risk" categories.

D. "Class D" - Minimal Risk: Data designed for public dissemination.

Data classified as Low Risk and Minimal Risk (and in some circumstances, Moderate Risk) are subject to disclosure. Requests for release of any of these data must be made and approved in accordance with the College's/States Public Records Policy.

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.

II. 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:

A. Data Trustee: Data trustees 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. Responsibilities include assigning data stewards, participating in establishing policies, and promoting data resource management for the good of the entire College.

B. 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.

C. Data Custodian: Information Technology Services (ITS) 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.

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.

Clarification and communication of roles in data classification are responsibilities of the Data Governance Committee.

Data Security Measures

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

I. Encryption requirements
II. Data protection and access control
III. Documented backup and recovery procedures
IV. Change control and process review
V. Data-retention requirements
VI. Data disposal
VII. Audit controls
VIII. Storage locations
IX. Data request processes and procedures
X. User awareness

Enforcement

ITS, in cooperation with other College authorities and administrators, will enforce this Policy, and establish standards, procedures, and protocols in support of the policy.

Any violation of this policy by a College student is subject to the Student Code of Conduct in the student handbook. For employees, any violation of this policy is "misconduct" under APO, CSO and faculty policies, including any appeal rights stated therein. Violations of law may also be referred for criminal or civil prosecution. Additionally, violations of this policy may result in termination or suspension of access, in whole or in part, to College information systems at the discretion of ITS where such action is reasonable to protect the College or the College information infrastructure.