POLICY 08:13:13
DATA CLASSIFICATION

I. Purpose

The purpose of this policy is to define the classification of data including the levels of classification and describing guidelines for access, use, and safeguarding of data, based on its level.

II. Scope

The following guidelines apply to data or information owned, created, collected or processed by Pellissippi State Community College. This policy applies to all individuals who access, use, or manage data owned by or protected by the college. This includes but is not limited to:

- Faculty, including adjunct faculty and temporary full-time faculty
- Staff, including full-time, temporary part-time and other contracted employees
- Student Employees
- Agents of the College
- Third party vendors that have been granted access to college resources

All parties with access to data on the college network or stored by the college should be familiar with this policy.

III. Definitions

Data custodian: The full definition and identification of data custodians at the college can be found in the Data Standards Manual linked from the Institutional Effectiveness, Assessment and Planning site. In summary, a data custodian is an administrator of a Pellissippi State office or division or his or her designee who may make data within his/her charge available to others for the use and support of the office or division’s functions and is responsible for the accuracy and completeness of data files in their areas and ensures the protection requirements are met before granting access to the data.

Data user: Any member of the college community that has access to college data, and thus is entrusted with the protection of that data.

IV. Policy

A. Data Classification

Data is organized into three distinct classes:

1. Restricted Data
2. Confidential Data
3. Public Data

Each class of data has its own requirements with respect to safeguards and procedures in the event of inappropriate disclosure.

1. Restricted Data

Restricted Data is defined as data, in any format, that is *regulated* by law or contract. Regular audits of access to Restricted Data should be conducted by the data custodians and appropriate control measures are implemented by data custodians.

Regulated Data Elements can include:

- Social Security Number (PII)
- Driver's License ID Number (PII)
- Passport ID Number (PII)
- Tax ID Number (PII)
- Health Information (HIPAA)
- Class Schedules (FERPA)
- Academic Actions (FERPA)
- Grades and Transcripts (FERPA)
- Payment Card Data (PCI)

Other data elements that can be associated with an individual (PII), particularly when used in various combinations with regulated data elements, may be treated as Restricted Data, depending on the usage. It is the responsibility of the data custodian to analyze each data set to determine if any given combination poses a risk.

Examples of Associated (PII) Data Elements

- Name
- Date of Birth
- Home Address
- Telephone Number

Safeguards for restricted data should include an approved storage location and regular monitoring and auditing of access to restricted data. Additionally, access should be limited to only those who have a legitimate need to use the data. Transmission of restricted data outside of the college's enterprise storage location requires both encryption and verification of the identities of the recipient. Any restricted data transmission should be done so that the data cannot be modified. Restricted data should not be stored unencrypted in a cloud solution and never stored in a non-college provided or contracted cloud solution. Restricted data should have a retention timeline and should be destroyed when no longer in use and when legally permissible. Data custodians and information technology staff will work together to ensure appropriate technologies are in place to provide adequate protections while ensuring availability for appropriate use.

2. Confidential Data

   Confidential data is not protected by state or federal law. However, its loss or unauthorized use could impair the college functions, cause significant financial or reputational loss or possibly lead to legal liability. Regular audits of access to Confidential data should be conducted by the data custodians to ensure appropriate access controls exist and access should be limited to only those who have a legitimate need to use or know the data. Transmission of confidential data outside of the college network requires both encryption and verification of the identities of the recipient. Confidential data should not be stored unencrypted in any cloud solutions, particularly those not contracted by the institution. By default, all institutional data that is not explicitly classified as Restricted or Public data should be treated as Confidential data. A reasonable level of security controls should be applied to Confidential data.

Examples of Confidential Data include but are not limited to:

- Account Credentials
- Payroll and Employment Documentation
- Donation/Giving History
- Systems & Network Diagrams
- Exams and Quizzes (questions and answers)

3. Public Data

Public data is any data that does not fall into the other classes. Public data does not pose a risk to the institution and may be publicly accessible but does not require public access. There are no restrictions on the storage or distribution of public data.

Examples of Public Data include but are not limited to:

- Public Web Sites/College Social Media accounts
- Directory Information
- Course Catalog
- Marketing Materials
- Job opening announcements
- Press Releases

B. Data custodianship

Each data set will have an identified data custodian(s). Data custodians are responsible for classifying the data and assigning the correct level of access to the data. Data custodians must ensure that the policy is enforced for their data set, and that the appropriate confidentiality, integrity and availability of the data are maintained. Currently, most data custodian responsibilities are provided by functional area leads and members of the Banner Steering Committee.

The data custodianship function shall have one or more data custodians assigned to each data set. These sets belong to major categories of institutional data, including:

- Financial data (institutional, student)
- Employment data (faculty, staff, student)
- Academic data (student, prospective student, faculty)
- Health data (student)
- Philanthropic data (alumni, donors)
- Security data (IT security configurations, physical security data)

Individuals with access to data have been granted a level of trust by the data custodians and are responsible for upholding the security and integrity of the data to which they have access, and should be aware of best practices in secure data management

As data are developed, data custodians assure that storage of, and access to, the data is appropriately managed. This includes the documentation and classification of all forms, views, reports and all other forms of access in which this data is made visible.

C. Data Classification and Usage Responsibilities

1. Data custodians are responsible for appropriately classifying data, documenting the business rules of their area and adhering to the data standards of the college. They will monitor the quality of the data input and output from the systems they use and work with other data custodians on integration requirements. They will work with data protection providers in regularly auditing appropriate data access for approved users.
2. Data users are responsible for complying with data use requirements
3. Data protection is provided by information technology personnel charged with applying the appropriate classification and enforcing the appropriate safeguards.

D. Auditing

To protect confidential data, designated information technology staff may use auditing technologies to scan institutional technology systems. These technologies may include programs and utilities that allow for programmatic inspection of data and access permissions. The results of these scans may be centrally correlated for analysis in a secure environment. These technologies are not to be used to read the full context of the data, but rather to match established patterns, such as SSNs, Payment Card Data, etc. Information obtained through auditing will be considered confidential data and restricted to appropriate personnel.

Reviewed/Recommended: President’s Council, March 6, 2017
Approved: President L. Anthony Wise Jr., March 6, 2017
Reviewed/Recommended: President’s Council, September 18, 2017
Approved: President L. Anthony Wise Jr., September 18, 2017