Pennsylvania College of Technology

Policy Statement

Title: Data Classification Policy

Number: P 8.04

Approved by:
Presidential Action

Approved Date: 11/01/2022
Implementation Date: 11/2022
Last Review Date: 11/2022
Last Revision Date: 11/2022

Persons/Departments Affected:
All Employees and Students

Responsible Department:
Information Technology Services

Definitions:
Data - Information that has been translated into a form that can efficiently be stored, transmitted, or processed by IT resources.

Policy:

I. PURPOSE

The purpose of this policy is to define the data classification requirements for information assets and to ensure that data is secured and handled according to its sensitivity and impact that theft, corruption, loss, or exposure would have on the institution. This policy provides direction to the institution regarding identification, classification, and handling of information assets.

II. SCOPE

The scope of this policy includes all information assets governed by Pennsylvania College of Technology. All faculty, staff and third parties who have access to or utilize information assets to process, store and/or transmit information for or on the behalf of Pennsylvania College of Technology shall be subject to these requirements.

III. POLICY

Pennsylvania College of Technology has established the requirements enumerated below regarding the classification of data to protect the institution’s information.

a. DATA OWNERSHIP AND ACCOUNTABILITY

Data owners are identified as the individuals, roles, or committees primarily responsible for information assets. These individuals are responsible for:

i. Identifying the institution’s information assets under their areas of supervision.

ii. Maintaining an accurate and complete inventory for data classification and handling purposes.

iii. Data owners are accountable for ensuring that their information assets receive an initial classification upon creation and a re-classification whenever reasonable. Re-classification of an information asset should be performed by the asset owners whenever the asset is significantly modified. Additionally, data owners are responsible for reporting deficiencies in security controls to management.

b. DATA CLASSIFICATION
Classification of data will be performed by the data asset owner based on the specific, finite criteria. Refer to the Data Classification and Handling Procedure to determine how data should be classified. Data classifications will be defined as follows:

RESTRICTED - Information whose loss, corruption, or unauthorized disclosure would cause severe personal, financial, or reputational harm to the institution, institution staff or the constituents/people we serve. Federal or state breach notification would be required, identity or financial fraud, extreme revenue loss, or the unavailability of extremely critical systems or services would occur. Common examples include, but are not limited to, some elements of Family Educational Rights and Privacy Act (FERPA) data, social security number, banking and health information, payment card information and information systems' authentication data.

PRIVATE – Information whose loss, corruption, or unauthorized disclosure would likely cause limited personal, financial, or reputational harm to the institution, institution staff or the constituents/people we serve. Federal or state breach notification would not be required, limited identity theft and very little revenue loss would occur, and the availability of critical systems would not be affected. Common examples include, but are not limited to, some data elements found in HR employment records, unpublished research data, and passport and visa numbers.

PUBLIC – Information whose loss, corruption, or unauthorized disclosure would cause minimal or no personal, financial, or reputational harm to the institution, institution staff or the constituents/people we serve. Common examples include, but are not limited sales and marketing strategies, promotional information, published research data, and policies.

c. DIRECTORY INFORMATION

i. ACADEMIC PERSONNEL AND STAFF DIRECTORY INFORMATION

Academic Personnel and Staff Director Information is defined as the following:

Name

Date of hire
Date of separation
Current position title
Employment status
Department of assignment, including office telephone number and office address

ii. STUDENT DIRECTORY INFORMATION

Student Directory Information is defined as the following:

Name of student
Telephone number
Email address
Class level
Dates of attendance
Major field of study
Number of course units in which student is enrolled
Degrees and honors received
Last school attended
Participation in official student activities
For intercollegiate athletic team members only:
Name
Height
Weight

d. DATA HANDLING

Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention policies and destruction methods. The specific methods must be described in the Data Classification Procedure.

e. RE-CLASSIFICATION

A re-evaluation of classified data assets will be performed at least once per year by the responsible data owners. Re-classification of data assets should be considered whenever the data asset is modified, retired, or destroyed.

f. CLASSIFICATION INHERITANCE

Logical or physical assets that “contain” a data asset may inherit classification from the data asset(s) contained therein. In these cases, the inherited classification shall be the highest classification of all contained data assets.

IV. ENFORCEMENT

Users who violate this policy may be denied access to the institution’s resources and may be subject to penalties and disciplinary action both within and outside of the institution. The institution may temporarily suspend or block access to an account prior to the initiation or completion of such procedures, when it appears reasonably necessary to do so to protect the integrity, security or functionality of the institution or other computing resources or to protect the institution from liability.

V. EXCEPTIONS

Exceptions to this policy must be approved in advance by the Chief Information Officer, at the request of the responsible data asset owner. Approved exceptions must be reviewed and re-approved by the asset owner annually.

VI. REFERENCES

Federal Information Processing Standard Publication 199 (FIPS-199)
NIST Special Publication 800-53 r4

Revision History:

Date:
Date:
Date:

Cross References:

Acceptable Use Policy P 8.03
Information Security Policy P 8.02