Purpose

This policy outlines the categories of data at Plaza College and establishes a structured framework for classifying institutional data based on its sensitivity, importance, and criticality to the College's operations.

Data Governance

Data governance at Plaza College is centered on enhancing data quality, securing access to information, developing shared definitions, managing metadata, and establishing comprehensive data-related policies. Institutional data is a vital institutional resource that must be safeguarded accordingly. Accurate and reliable data is essential for informed decision-making across all levels of the College. Effective governance ensures transparency and instills confidence in faculty, staff, and leadership to rely on institutional data for both strategic planning and daily operations.

Managing Institutional Data

The following guiding principles serve as foundational standards for managing and using institutional data responsibly:

- All institutional data is owned by Plaza College and treated as a critical asset.
- Redundant or unnecessary replication of institutional data is discouraged.
- Institutional data must be secured appropriately.
- Access to institutional data must align with predefined roles and business needs.
- Those responsible for data must be held accountable for their designated roles.
- Ongoing data maintenance procedures must be clearly defined.
- Any disputes or issues involving institutional data must follow an established resolution process.
- Each data steward is accountable for the data subset within their scope.

Roles Involved in Data Oversight

While no single person or department "owns" institutional data, several defined roles govern access, responsibility, and accountability:

- Technology Committee: This group consists of cross-functional representatives from across Plaza College, including leaders of major departments. The committee, co-chaired by the Provost and Chief Information Officer, oversees all technological initiatives at the College, including data governance.
- Data Stewards are operational-level IT management responsible for specific categories of institutional data. They have the authority to manage and make decisions about the data they oversee.

- Data Trustees: These are senior administrators—such as deans and department heads—who hold policy-level authority over the definitions, usage, and access protocols for institutional data. Trustees assign stewards to specific subject areas.
- Data Custodians: Custodians are IT Support staff who manage the systems and infrastructure that store and process institutional data.
- Data Users: Individuals or departments at Plaza College who are granted access to institutional data to fulfill their official responsibilities. This access is granted solely for business or academic purposes.

  Related supporting documents include the Data Classification Policy and accompanying Data Classification Guidelines.

Data Classification

Data classification refers to the process of categorizing information based on its confidentiality and the potential risk to Plaza College if the data were to be accessed, modified, or deleted without permission. Classification helps determine the appropriate baseline security controls required to protect each data category. Institutional data falls into one of three classifications:

Restricted Data

Data should be designated as Restricted if its unauthorized access, modification, or destruction could result in serious harm to Plaza College or those it serves. This category demands the highest level of security. It includes any personally identifiable information (PII) or other regulated data subject to local, state, or federal privacy laws such as:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standards (PCI DSS)

Private Data

Private data includes information that, if improperly accessed or altered, could pose a moderate risk to Plaza College or its affiliates. Data not explicitly categorized as Public or Restricted should be treated as Private by default. Reasonable safeguards should be applied to this classification. Examples include financial records, contract negotiations, and employee compensation.

Public Data

Public data is information that can be disclosed, changed, or deleted with minimal or no adverse impact on Plaza College. While this type of data does not require strong confidentiality measures, protections must still exist to prevent unauthorized alteration or deletion. Examples include publicly shared course catalogs, news releases, or other data made available to the general public.

Default Classification Guidelines

Any data that includes PII or is governed by regulatory requirements is, by default, considered Restricted. All other institutional data should default to Private unless otherwise determined.

Applicable Privacy Laws and Regulations

FERPA is a federal law that safeguards the privacy of student education records. It applies to institutions receiving funding from the U.S. Department of Education. FERPA grants students the right to review their educational records, request corrections, and restrict certain disclosures. Schools must obtain written permission before releasing non-directory information. Violations may result in the loss of federal financial aid and other funding.

More information is available online.

GLBA (The Gramm-Leach-Bliley Act) mandates financial institutions to protect customers' personal financial data. It requires transparency about data collection, use, and safeguards. Penalties for noncompliance include fines of up to $100,000 per institution and $10,000 for responsible individuals.

More information is available online.

HIPAA regulates the use and disclosure of Protected Health Information (PHI), covering medical history, health care provision, and payment records. Wrongful disclosures carry penalties ranging from $50,000 to $250,000 in fines and prison terms of one to ten years, depending on severity. These penalties apply to individuals, not just institutions.

More information is available online.

Payment Card Industry Data Security Standards (PCI DSS)

PCI DSS (The Payment Card Industry Data Security Standard) governs how businesses handle credit card data. Organizations that accept credit cards must secure their networks and follow standardized procedures. Noncompliance can lead to penalties of up to $500,000 per data breach and loss of the ability to accept card payments.

More information is available online.