PimaCountyCommunityCollegeDistrict
Administrative Procedure

AP Title:	**Information Management Standard**
AP Number:	AP 9.01.08
Adoption Date:	3/13/19
Schedule for Review & Update:	Every three years
Review Date(s):	3/25/19, 6/14/23
Revision Date(s):	6/14/23
Sponsoring Unit/Department:	Information Technology
Policy Title(s) & No(s).:	Information Technology Resource Management, BP 9.01
Legal Reference:	
Cross Reference:	Records and Information Management, AP 2.15.01, Data and Classification Handling Handbook, College Records Handbook

PURPOSE

The purpose of this Administrative Procedure (AP) is to protect Pima Community College ("College") information resources from accidental or intentional unauthorized access, modification, or damage, while also preserving the open information sharing requirements of its academic culture. The College policy is to comply with all applicable legislative, regulatory, and contractual requirements concerning information security. College information security standards may exceed legally prescribed requirements.

SECTION 1: Policy Statement

Information that the College or its agents use in the course of conducting College business is an institutional resource. Although individuals, offices, departments or

programs may have responsibilities for creating and maintaining portions of College information, the College itself retains ownership of and responsibility for the information.

This AP applies to faculty, staff, and others granted use of College information or related assets and defines their responsibility for the protection and appropriate use of College information, applications, computer systems, and networks.

SECTION 2: Definitions

Data, Information Asset, Record	These are all interchangeable terms that mean the following: Any recorded information generated or received in the course of conducting business, AND which must be maintained to meet the fiscal, legal, historical, or administrative needs of the organization and maintained in any medium and repository.
Department Data Plan	A Data/File plan differs from office to office, but it consists of: • Description of the kinds of documents or data identified to be records • The classification of the records into range of categories • Details about the location of the stored records • Description of the retention schedule and period • Makes the distinction and assigns the responsibility for maintaining records to that specific office • Establishes data handling guidelines for that specific record set
Data Steward	Data Stewards are the functional business owner of the data for the College (typically a Director level position) and will:

- Assign information under their stewardship to one of four security classifications: public, internal, confidential, or regulated based upon the information's intended use and the expected impact if disclosed.
- Bear primary responsibility for decisions regarding data usage and handling for the data under their stewardship.
- Coordinate activities with areas outside their own when data usage, access, and/or handling impacts extend beyond their own unit.

SECTION 3: Procedure

College departments shall comply with safeguards established within this policy. The management of information assets is the responsibility of the owner, or creator of the data (records). Information Technology Security will work with department leadership to develop:

- Data Asset Inventory in support of AP 2.15.01
- Departmental Data Plan with Data Classification
- Data Handling Standards
- Information Management Section within a departmental operations manual
- Vendor Functional Requirements for storing College information assets
- Training
- Security Awareness

All College departments shall ensure they have a Departmental Data Plan and Data security measures must be implemented commensurate with the sensitivity of the data and the risk to the College if the data is compromised. It is the responsibility of the applicable steward (functional owner) of the data to evaluate and classify data for which they are responsible, according to the classification system adopted by the College and structure described below:

	PUBLIC	INTERNAL USE	CONFIDENTIAL	REGULATED
DESCRIPTION	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally. · NO DAMAGE would occur if Public information were to become available to parties either internal or external to Pima Community College. · Impact would not be damaging or a risk to business operations.	Internal Use information is information originated or owned by Pima Community College or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests. · **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to Pima Community College. · Impact could include damaging the company's reputation and violating contractual requirements.	Confidential information is highly-valuable, sensitive business information and the level of protection is dictated internally by Pima Community College. · **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to Pima Community College. · Impact could include negatively affecting Pima Community College's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.	Regulated information is highly-valuable, highly-sensitive business information, and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need. · **SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to Pima Community College. · Impact could include negatively affecting Pima Community College's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.

Specific instructions on data handling are located in the College's Data Classification and Handling Guidelines.

SECTION 4: Policy Enforcement

Levels of compliance will be reported annually to the appropriate College governance bodies.