PimaCountyCommunityCollegeDistrict
Administrative Procedure

AP Title:	**Gramm-Leach-Bliley Act Information Security Plan**
AP Number:	AP 9.01.09
Adoption Date:	5/8/24
Schedule for Review & Update:	Every three years
Review Date(s):	
Revision Date(s):	
Sponsoring Unit/Department:	Information Technology
Policy Title(s) & No(s).:	Information Technology Resource Management, BP 9.01
Legal Reference:	U.S. Department of Education Program Participation Agreement (PPA); Gramm-Leach-Bliley Act (15 U.S. Code § 6801), 32 C.F.R. Part 2002; Arizona State Statutes: §18-552; §18-606 and §18-609[SV2]; Part 314 - Standards for Safeguarding Customer Information
Cross Reference:	Written Information Security Program; AP 9.01.03 Security of the Information Technology Infrastructure; AP 9.01.01 Acceptable Use of Information Technology Resources

PURPOSE

Pima Community College will protect, to the extent reasonably possible, the privacy, security, and confidentiality of personally identifiable financial records and information. This Administrative Procedure (AP) applies to all personally identifiable financial records and information and covers employees and all other individuals or entities using these records and information for any reason. This AP

also establishes an expectation that members of the College community act in accordance with this policy, relevant laws, contractual obligations, and the highest standards of ethics.

SECTION 1: Definitions

Customer - means any individual (past or present) who receives financial service from the College. Customers may include students and those attempting to become students, parents, spouses, all employees, and third parties.

Protected information - means any personally identifiable financial or other personal information, not otherwise publicly available, that the College has obtained from a customer in the process of offering a financial product or service; such information provided to the College by another financial institution; such information otherwise obtained by the College in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

SECTION 2: Procedure and Responsibilities

2.1. The College's Assistant Vice Chancellor for Information Technology is responsible for establishing and maintaining the College's Written Information Security Program (WISP), in compliance with the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), 15 U.S. Code Section 6801.

2.2. The Written Information Security Program (WISP) is designed to provide the following safeguards:

2.2.1. Protect the security and confidentiality of protected information.

2.2.2. Protect against anticipated threats or hazards to the security or integrity of such information.

2.2.3. Protect against unauthorized access to, or use of, protected information that could result in substantial harm or inconvenience to any customer.

2.3 The Written Information Security Program (WISP) also provides mechanisms to:

2.3.1. Identify and assess risks that may threaten protected information maintained by Pima Community College.

2.3.2. Designate employees responsible for coordinating the program.

2.3.3. Design and implement safeguards specific to the program.

2.3.4. Manage the selection of service providers.

2.3.5. Modify the WISP to reflect changes in technology, the sensitivity of protected information, and overall threats to information security.

2.3.6. Reference related policies and procedures.

2.3.7. Develop a plan to respond to any security incident involving a breach of security.