PimaCountyCommunityCollegeDistrict
Administrative Procedure

INTERIM — EFFECTIVE JULY 31, 2026

AP Title:	**Security Awareness Training**
AP Number:	AP 9.01.13
Adoption Date:	Interim – July 24, 2026
Schedule for Review & Update:	Every five 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:	Gramm-Leach-Bliley Act (GLBA) 15 U.S. Code § 6801; Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g
Cross Reference:	Written Information Security Program (WISP), AP 9.01.09; Acceptable Use for Technology Resources, AP 9.01.01

PURPOSE

The purpose of this Administrative Procedure (AP) is to establish a comprehensive and accountable Cybersecurity Awareness Training program for Pima Community College (PCC or the College). This AP aligns with industry best practices and regulatory compliance frameworks, ensuring that all members of the College community understand their responsibility to protect the confidentiality, integrity, and availability of the College's information technology (IT) resources and sensitive data.

Cybersecurity threats are always evolving, and human error is a major weakness. That is why ongoing training is crucial for the College's security. Promoting a security-minded culture helps lower risks, meet legal requirements, and protect the information of students, faculty, and staff.

SCOPE

This policy applies to all users granted access to College IT resources, networks, systems, and email accounts. This includes employees, contractors, and volunteers (collectively, “Users”).

SECTION 1: Roles and Responsibilities

1.1 Information Technology Responsibility

1.1.1. The College's Information Technology department, under the direction of the Assistant Vice Chancellor for Information Technology and Chief Information Security Officer (CISO), is responsible for designing, delivering, and administering an accountable institutional cybersecurity training program. IT shall:

1.1.1.1. Select and deliver training that aligns with industry best practices (e.g., NIST, SANS) and addresses threat landscapes (e.g., phishing, ransomware, social engineering).

1.1.1.2. Track compliance, monitor participation rates, and maintain records of training completion.

1.2 Supervisor and Leadership Responsibility

1.2.1 Supervisors are responsible for ensuring that their direct reports complete assigned training modules.

1.3 User Responsibility

1.3.1 Every individual granted access to PCC technology resources is responsible for completing cybersecurity awareness training as a condition of obtaining and retaining network access.

SECTION 2: Training Requirements

2.1 Ongoing Awareness Training

2.1.1 **Training Program:** The IT department determines the frequency, distribution, and subject matter of the training based on current threat vectors, organizational risk, and regulatory mandates.

2.1.2 **Completion Deadlines:** Each assigned training will carry a specific completion deadline. Users must successfully complete the training within the specified timeframe to maintain good standing.

2.2 Targeted or Remedial Training

2.2.1 IT reserves the right to mandate specialized training for employees who handle highly sensitive data (e.g., Financial Aid, Registrar, Fiscal Services) or remedial training for individuals who demonstrate difficulty identifying security threats (e.g., repeatedly failing simulated internal phishing exercises).

SECTION 3: Program Accountability

3.1 Accountable Performance

3.1.1 Cybersecurity training is a mandatory duty.

3.1.2 Repeated failure to comply with training requirements constitutes a violation of College policy and is subject to disciplinary action in accordance with applicable College personnel policies, Employee Handbooks, and Codes of Conduct.

SECTION 4: Program Evaluation and Updates

4.1 Continuous Improvement

4.1.1 IT will review training data, simulated phishing metrics, and emerging global threat intelligence annually to continuously update training modules, ensuring the curriculum reflects modern security threats.