PimaCountyCommunityCollegeDistrict
Administrative Procedure

AP Title:	**Acceptable Use of Information Technology Resources**
AP Number:	AP 9.01.01
Adoption Date:	11/13/06
Schedule for Review & Update:	Every three years
Review Date(s):	5/1/15, 5/20/21, 5/8/24
Revision Date(s):	5/1/15, 5/20/21, 5/8/24
Sponsoring Unit/Department:	Information Technology
Policy Title(s) & No(s).:	Information Technology Resource Management, BP 9.01
Legal Reference:	
Cross Reference:	

PURPOSE

The purpose of this Administrative Procedure ("AP") is to define and authorize the process of creating and enforcing Acceptable Use Standards for Pima Community College ("College") information technology ("IT") resources. This AP applies to all College employees, students, visitors, volunteers, and any other authorized users of College IT resources.

SECTION 1: Definitions

"Cloud Services" shall mean such service models as defined within NIST SP800-145, further included within FedRAMP v.4.2 at p.3 as part of the College's Information Technology Resources.

"College IT Resources" include all computer and network systems, software, hardware, services, mobile devices, and audiovisual equipment, and Cloud

Services owned and operated by, or operated for, the College and/or connected to College equipment.

SECTION 2: Acceptable Use Agreement

2.1 For All Users of College IT Resources

2.1.1 The Assistant Vice Chancellor for Information Technology is responsible for creating and disseminating an Acceptable Use Agreement ("Agreement") applicable to all users of College IT Resources, including, but not limited to, all College employees, students, volunteers, visitors, and community members.

2.1.2 The Agreement shall specify that any and all individuals who access, connect to, or otherwise utilize College IT Resources shall be deemed to have read, understood, and agreed to abide by the terms of the Agreement.

2.1.3 The Agreement shall be reviewed and updated as necessary not less than every three (3) years, and more frequently as needed, by the Assistant Vice Chancellor for Information Technology. Mid-cycle changes will be maintained on the College's Intranet until added to the Agreement.

2.2 Signature Required for College Employees

2.2.1 All new College employees must sign the Agreement before they are given access to College IT Resources. Each employee's signed Agreement shall be kept on file with the College's Human Resources Office.

2.2.2 The College's Assistant Vice Chancellor for Human Resources (Chief Human Resources Officer) is responsible for ensuring employees sign the Agreement, as well as for maintaining records of signed Agreements and taking appropriate action in the event employees fail to sign the Agreement, including, but not limited to, revoking access to IT resources.

Acceptable Use of Information Technology Resources
Pima Community College

I. Purpose

A. The purpose of this policy ("Policy") is to establish the requirements for the use of all technology, computing, and network resources at Pima Community College ("PCC").

B. Pima Community College ("PCC" or "College") is dedicated to providing affordable, comprehensive educational opportunities that support student success. To accomplish these aims, the College has developed and provides multiple technologies and systems. It is the responsibility of all users of these systems to respect the rights of other users, to protect the integrity of PCC systems, and to comply with all pertinent license and contractual agreements.

II. Scope

A. This Policy applies to everyone who uses PCC technology or technology on behalf of PCC, whether it is used locally or remotely, including all PCC faculty, staff, students, visitors, contractors, consultants, and anyone who connects to or uses PCC systems or networks ("Users"). All Users are required and presumed to know and comply with all applicable laws, policies, and rules governing the use of PCC Technology.

B. PCC Technology includes all College-owned, -licensed, or -managed hardware, including, without limitation, servers, desktop computers, laptop computers, tablet devices, mobile phones or other mobile web-enabled devices, telephones, and facsimile machines; software, data files, network drives, communications systems, and any data transferred through the College's physical or wireless network, regardless ownership or affiliation.

C. PCC Technology also includes any and all technology administered or developed by anyone employed by or representing the College, including all applications, data, and services (*e.g.*, web sites and software developed for or representing PCC and its constituents.

III. Acceptable Use Requirements

A. Users may only utilize and/or access PCC Technology for which they have the proper authorization. Users will only have access to the systems and information deemed necessary to perform essential job duties.

B. Users should make reasonable efforts to protect their logon information and passwords and to otherwise secure PCC Technology against unauthorized access, including enabling and utilizing security features on all computers, mobile phones, tablets, and other devices.

C. Users may not use or attempt to gain access to another User's PCC Technology or attempt to obtain another User's logon name or password without proper authorization.

D. Each User is personally responsible for the appropriate use of all PCC Technology assigned to the User or to which the User has authorized access.

E. Users will be accountable for any misuse or unauthorized access of the PCC Technology assigned to them. Users may not enable unauthorized persons to access the PCC network by using a PCC computer or a personal computer that is connected to the PCC network. Any such misuse or unauthorized access may result in disciplinary action for the User.

F. Users are expected to comply with all contractual and licensing agreements respecting certain third-party resources by which PCC is bound.

G. Users must comply with any additional requirements, policies, or guidelines established for specific PCC Technology to which the User has been granted access. When additional requirements, policies, and guidelines, are more restrictive than this Policy, the more restrictive requirements, policies, or guidelines will take precedence.

H. Users must not use PCC Technology in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software, or hardware components of a system.

I. If a PCC employee uses a personally owned device to access PCC Technology or conduct PCC business, he or she shall abide by this Policy and all other applicable PCC policies and administrative procedures. Users should bear in mind that any such use of a personally owned device may subject the contents of that device and any communications sent or received on it to disclosure pursuant to a lawful subpoena or public records request.

J. In addition to the forgoing general requirements, the following specific uses of PCC Technology are expressly prohibited:

1. Use of a non-PCC-issued email service or online storage service for conducting PCC business unless use of the non-PCC service has been expressly authorized in writing by PCC's Assistant Vice Chancellor for Information Technology or his or her designee;

2. Sharing one's assigned online services account information, passwords, or other information used for identification and authorization purposes with other Users without authorization;

3. Developing or establishing Internet technologies and services that serve or represent PCC without proper authorization or in violation of other PCC policies and regulatory requirements;

4. Accessing, posting, displaying, transmitting, or otherwise using material that is discriminatory, defamatory, obscene, sexually explicit, harassing, intimidating, threatening, or disruptive;

5. Disclosing or in any way causing to be disclosed confidential or sensitive College, employee, or student information without prior authorization;

6. Engaging in personal commercial or other for-profit activities without prior authorization.

7. Using PCC Technology for personal political activity or to engage in political lobbying on behalf of PCC without authorization;

8. Infringing on copyright, license, trademark, patent, or other intellectual property rights;

9. Intentionally disrupting or harming PCC Technology or other College operations, including, without limitation, destroying College equipment, placing a virus on College computers, adding or removing a Computer program without authorization, changing settings on shared computers without authorization, or removing data from PCC Technology without authorization;

10. Installing or using unauthorized software on PCC Technology;

11. Storing PCC records in any form in an unsecured or unapproved location, or on an unsecured or unapproved system without authorization;

12. Engaging in or promoting illegal activities;

13. Violating any PCC policy or administrative procedure;

14. Gaining unauthorized access to the data files or equipment of others, accessing electronic resources by using another person's name or electronic identification, or sending anonymous electronic communications.

IV. Privacy and Monitoring

A. While the College recognizes the importance of privacy in an institution of higher learning and will endeavor to honor that ideal, Users should have no expectation of privacy in any information stored on or sent through PCC Technology or personal devices connected to PCC Technology, except as required by law. Users should note that electronically stored information of any kind may be discoverable in a legal action or accessed and reviewed during the course of a PCC administrative investigation.

B. All PCC Technology and the work, data, and other material stored on it in any form is subject to review, monitoring, blocking, or removal by PCC, as well as other maintenance and protective actions, such as logging, deleting, encrypting or decrypting, threat analysis, performance analysis, backup, and troubleshooting. All such actions are within the authority of PCC's administration.

V. Record Retention and Destruction

A. Any electronically stored information generated or received by a PCC employee which constitutes a PCC or PCC-student record shall be classified, retained, and destroyed in accordance with administrative procedure 2.15.01 or other applicable policies and regulations addressing the retention of college or student records. In addition, all PCC records must be maintained in an approved repository within the College's jurisdiction.

B. Storing PCC and PCC-student records in any medium on unsecured or unapproved systems is a violation of PCC policy as defined in Administrative Procedure 2.15.01.

VI. Data Security and Classification

A. It is the responsibility of the applicable data custodian to evaluate and classify data for which he/she is responsible according to the classification system adopted by the College and described in the Data Classification Standard Guide.

VII. Administrator Rights

A. Administrator rights will only be granted under the condition that they are essential for the performance of the grantee's job. The process to obtain administrator rights is a highly controlled and restricted process.

VIII. Remote Access

A. Personal devices are not permitted to connect to the College's network via VPN. Personal devices are permitted to access resources available over the Internet.

B. Employees, contractors, and temporary staff will make no modifications of any kind to the remote access connection without the express approval of Pima Community College's IT department. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations, etc.

C. Employees, contractors, and temporary staff with remote access privileges must ensure that their computers are not connected to any other network while connected to Pima Community College's network via remote access, with the obvious exception of Internet connectivity.

D. If a College-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their manager and Pima Community College's IT department immediately.

E. The remote access user also agrees to immediately report to their manager and Pima Community College's IT department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

F. The remote access user also agrees to and accepts that his or her access and/or connection to Pima Community College's networks may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity. This is done to identify accounts/computers that may have been compromised by external parties.

G. By default, employees are not granted remote access. Employees must go through the appropriate process to request remote access.

IX. Investigations & Discipline

A. For Employees**:** Use of PCC Technology is subject to the Code of Conduct section of the Employee Handbook. Misconduct will be investigated in accordance with AP 9.01.07. Unauthorized use or abuse of PCC Technology by PCC employees may result in disciplinary action up to and including termination of PCC employment.

B. For Students: Use of PCC Technology is subject to the Student Code of Conduct. Unauthorized use or abuse of PCC Technology by PCC students may result in disciplinary action up to and including expulsion from the College.

C. For All Users: The misuse or abuse of PCC Technology may also violate state or federal law and may result in additional civil or criminal liability and/or penalties.

X. Legal Standards

All Users of PCC Technology are expected to abide by all Federal and State laws and regulations. The following list of relevant statutes is used for illustrative purposes, and is not intended to be a comprehensive guide to Federal and/or State law:

- FERPA (Family Educational Rights and Privacy Act): regulates the confidentiality of student records.
- GLBA (Graham Leach Bliley Act): regulates the confidentiality of financial information.
- HIPAA (Health Insurance Portability and Accountability Act): regulations the security and privacy of heath information.
- PCI DSS (Payment Card Industry Data Security Standard): regulates the confidentiality of credit card information.
- DMCA 1998 (Digital Millennium Copyright Act): regulates the protection of intellectual property.
- USC Title 18 §1030 (United States Code: Fraud and related activity in connection with computers)
- ARS 13-2008 (Arizona State Law: Taking identity of another person or entity) prohibits identity theft.
- ARS 13-2316 (Arizona State Law: Computer tampering; venue; forfeiture): prohibits unauthorized use of computers.
- ARS 13-2407 (Arizona State Law: Tampering with a public record): regulates the integrity of PCC Data.
- ARS 13-3001-3019 (Arizona State Law: Eavesdropping and Communications): prohibits forgery and eavesdropping.
- ARS 13-3707 (Arizona State Law: Telecommunication fraud): prohibits telecommunication fraud.
- ARS 38-448: (Arizona State Law: Access to Pornography is Prohibited): prohibits access to pornography by PCC employees on PCC Systems.
- ARS 38-501-511 (Arizona State Law: Conflict of Interest): prohibits use of PCC resources regarding conflicting interests.
- ARS 44-1372 (Arizona State Law: Commercial Electronic E-mail): prohibits spam.
- ARS 44-1373-1373.03 (Arizona State Law: Confidentiality of Personal Identifying Information) regulates the protection of personal identifying information.

I have read and agree to abide by the above standards and acknowledge that any action by me which is contrary to the above standards may be cause for discipline, discharge or legal action against me.

_____

Print Name

_____ _____

Signature Date