Acceptable Use Agreement

Acceptable Use of Information Technology Resources

Last Revised: December 12, 2024

I. Purpose

A. In accordance with Administrative Procedure ("AP") 9.01.01, the purpose of this Acceptable Use Agreement ("Agreement") 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 Agreement 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, Artificial Intelligence (AI) tools, and any data transferred through the College's physical or wireless network, regardless of 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. Full-time employees will be provided with a single device (laptop or desktop computer) based on their job duties. Employee requests for additional devices will require business justification.

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.

1. Password requirements will be defined by the Information Technology Department and shall follow the National Institute of Standards and Technologies (NIST) Special Publication 800-63B guidelines. For security and compliance purposes, the Information Technology Department may require you to periodically change your password.

2. Passwords shall be between 15 and 127 characters in length, must include at least one number and one letter, and may contain uppercase letters, lowercase letters, numbers, and special characters. Due to technology limitations, passwords may not contain a colon ":".

3. Passwords should avoid commonly used, predictable, easily guessed, or commonly breached/weak passwords.

4. Passwords should not be reused from account to account or recycled for the same account.

5. Accounts will be locked for 15 minutes after 5 consecutive failed attempts.

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 Agreement, 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 Agreement 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 (anything besides Google Drive) 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 AP 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 AP 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.

B. Pima Community College expressly forbids the disclosure of College data classified as Internal Use, Confidential, or Regulated; or the distribution of such data in any medium, except as required by an employee's job responsibilities. In this context, disclosure means giving the data to persons not previously authorized to have any type of access to it. Pima Community College also forbids the use of any College data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity. (See AP 9.01.08 for full definitions and examples of Internal Use, Confidential, and Regulated data).

C. Users are expected to protect personally identifiable information (PII) and other sensitive, classified, or personal data when using generative AI tools to avoid disclosing—or causing to be disclosed—such information about the College, its employees, its students, and the community.

VII. Administrator Rights

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. Prohibition of Circumventing Security Measures

A. All users are strictly prohibited from attempting to bypass, disable, or otherwise circumvent any security measures, controls, devices, or policies that have been implemented by Pima Community College. This includes, but is not limited to:

1. Tampering with Security Software: Attempting to disable, alter, or bypass any security software, such as antivirus programs, firewalls, intrusion detection/prevention systems, or endpoint protection platforms.

2. Manipulating System Attributes: Removing or altering system attributes or settings, such as file quarantine flags, security permissions, or other security-related metadata.

3. Unauthorized Access or Privilege Escalation: Gaining or attempting to gain unauthorized access to systems, applications, or data by circumventing access controls, using unauthorized tools, or exploiting vulnerabilities.

4. Evasion of Monitoring or Logging: Engaging in any activity designed to evade monitoring, logging, or auditing mechanisms implemented by the College.

5. Use of Unauthorized Tools or Software or Visiting Known Malicious Websites: Installing or using software, scripts, or tools intended to bypass security controls, including but not limited to the use of unauthorized VPNs, anonymizers, encryption tools, or tools designed to alter a digital footprint.

B. Users who attempt to install unauthorized software that attempts to bypass security measures during the installation process will be held accountable as though they personally attempted to bypass those security measures. By attempting to install unauthorized software, users are assuming responsibility for the actions taken by the installation package or installer.

C. Any attempt to circumvent security measures, regardless of intent, will be considered a serious violation of this policy, will be investigated, and may result in disciplinary action, up to and including termination of employment, legal action, restricted access to information resources, loss of access privileges, or another appropriate action as deemed by the outcome of the investigation.

X. Password Management

A. All employees and faculty will be issued a password manager to use for work-related password management.

B. The use of all other password/credential management solutions will be disabled on College-issued assets (e.g., built-in password managers in Chrome, Edge, Firefox, Safari, and Keychain Access).

C. All staff and faculty are strongly encouraged to use the College-issued password manager (“password manager”) for all work-related passwords.

1. The password manager should be used to automatically generate and store unique, complex passwords, thereby eliminating weak passwords, password reuse, and password fatigue.

2. The use of a password manager reduces the number of passwords a user has to remember to two: one to login to their device (i.e., logging into the PCC domain) and one to log into the password manager vault.

3. Where possible, generated passwords should be a minimum of 16 characters in length and include one from each of the following: uppercase, lowercase, numbers, and symbols.

4. The password for the password manager vault login will be a minimum of 20 characters in length and include one from each of the following: uppercase, lowercase, numbers, and symbols.

5. If a user cannot remember their password manager vault password, an administrator can reset the password for them. Administrators do not have the ability to recover this password. Administrator password resets will require **in-person** identity verification.

D. The password manager will be used in conjunction with DUO multifactor authentication (MFA).

E. The password manager will be the only authorized method for password sharing of shared logins or guest accounts.

1. When a password no longer needs to be shared, the sharing permissions should be removed, and the password should be changed.

Note: Service accounts managed by the College's Information Technology Department will continue to be managed through the department's existing policies and procedures.

F. The password manager should only be used from secure, institutionally approved devices that meet security requirements and standards.

G. While the password manager should only be used for work-related passwords, in the event a user stores personal passwords, users should export those items prior to departing the College. Upon separation from the College, users will lose access to the password manager.

H. Assistance with the password manager can be requested through the Information Technology Department Service Desk.

I. Security-related incidents (e.g., account compromise) shall be reported immediately to the Information Technology Department.

XI. Security Awareness Training

A. All users that are within scope of this acceptable use will be required to undergo information security awareness training administered by Pima Community College.

B. Users who are non-compliant may lose access to College systems.

C. A user may be considered non-compliant for the following reasons:

1. A user fails to complete the required security awareness training.
2. A user repeatedly fails simulated phishing assessments.
3. A user who continually fails in the ability to carry out expected actions from security awareness training.

XII. 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.

XIII. 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 16-1023 (Arizona State Law: Digital impersonation of candidate or other person; relief; applicability; definitions).

▪ ARS 16-1024 (Arizona State Law: Deepfakes; candidates; exemptions; civil liability; definitions).

▪ 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.

I further acknowledge and understand that I am required to review and abide by the standards set forth in AP 9.01.01 and in this Agreement, as well as any future revisions to AP 9.01.01 and/or this Agreement that PCC may issue.

____

Print Name

______________________________ _________________________

Signature Date