Chapter 3 - General Institution

AP 3720 ~~Use of Technology and Information Resources and Employee Acceptable Use Agreement~~ Acceptable Use of Technology and Information Resources [Title change to apply to all users as opposed to employees only.]

References:

~~Education Code Section 70902~~; Government Code Section 3543.1 subdivision (b); ~~17 U.S.C. § 101 et seq. (Copyright Act);~~ Penal Code Section 502; Cal. Const., Art. 1 Section 1; 15 U.S. Code Sections 6801 et seq.; 17 U.S. Code Sections 101 et seq.; 16 Code of Federal Regulations Parts 314.1 et seq.; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45 ~~Academic Senate for California Community Colleges 1999 paper *Academic Freedom, Privacy, Copyright and Fair Use in a Technological World*~~ **[Updated citations from CCLC.]**

The College~~'s~~ technology ~~systems~~ resources, including but not limited to software, hardware, and data, ~~and tools~~ are the sole property of Mt. San Antonio College. They may not be used by any person without the proper authorization of the College. The technology systems ~~and tools~~ resources are for College instructional and work-related purposes. College information resources should not be used for personal activities not related to appropriate College functions, except in a purely incidental manner so long as: (a) it does not consume more than a trivial amount of system resources; (b) it does not interfere with the productivity of other campus employees; and (c) it does not pre-empt any College activity. **[Changed 'District' to College'. Incidental use statement added by IT and edited for clarity by HR.]**

This procedure applies to all Mt. San Antonio College students, faculty, and staff and to others granted use of College information resources. This procedure refers to all College information resources whether individually controlled or shared, stand-alone, or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the College. This includes, but is not limited to, personal ~~computers~~ devices when used to access College information resources, workstations~~,~~ and associated peripherals, email, websites, ~~and~~ software, and information resources, regardless of whether used for administration, research, teaching, or other purposes. **[Updated language to cover all data irrespective of device, method, or modality of access.]**

Privacy

The College recognizes the privacy interests of faculty and staff and their rights to freedom of speech, participatory governance, and academic freedom, as well as their rights to engage in protected union and concerted activity. However, both the nature of electronic communication and the public character of College business make electronic communication less private than many users anticipate. In addition, the College Network may be subject to access by both internal and external users. For these

reasons, there are virtually no online activities or services that guarantee an absolute right of privacy, and therefore, the College Network is not to be relied upon as confidential or private. **[Added 'Privacy' section to clarify that there is no guarantee of privacy.**

~~Conditions of Use~~

~~Individual units within the College may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines, and/or restrictions. Employees must also consider the open nature of information transferred electronically and should not assume an absolute guarantee of privacy or restricted access to such information. Mt. San Antonio College reserves the right to monitor all use of the College network and computers to assure compliance with appropriate policies. Mt. San Antonio College will exercise this right only for legitimate College purposes including, but not limited to, ensuring compliance with this procedure and the integrity and security of the system.~~

~~The College supports and endorses the fundamental principles and the right of freedom of expression and endeavors to ensure appropriate confidentiality of communication. Nevertheless, all users should be aware that they have no guarantee of privacy or security when using College technology systems and tools. The College strives to provide the highest degree of privacy and security possible when transferring data but disclaims responsibility if security measures are circumvented and the information is compromised.~~
[Removed and replaced with 'Privacy' and 'Nondiscrimination' paragraphs below]

Nondiscrimination

All users have the right to be free from any conduct connected with the use of the Mt. San Antonio College network and computer resources that discriminates against any person on the basis of protected characteristics under Board Policy 3410. No user shall use the College network and computer resources to transmit any message, create any communication of any kind, or store information that violates any College procedure regarding discrimination or harassment, or that is defamatory or obscene, or that constitutes the unauthorized release of confidential information. **['Nondiscrimination' section added by HR due to past issues with harassment through digital means including but not limited to email.]**

Legal Process

~~This procedure exists within the framework of the College Board Policy and State and Federal laws. A user of College information resources who is found in violation of the College's computer use policies is subject to proper disciplinary action including the reporting of such activity to the appropriate authorities as required by law, up to and including, but not limited to, loss of information resources privileges; disciplinary suspension, or termination from employment or expulsion; and/or civil or criminal legal action (see Appendix A: Selected Examples of Unacceptable Use).~~

Technology users will comply with all Board Policies and Administrative Procedures for any specific set of resources to which access has been granted.

Users of College technology ~~systems~~ **resources** ~~and tools~~ should also be aware of items such as the following:

- Possibility of Disclosure - Users must be aware of the possibility of unintended disclosure of communications.

- **Retrieval - It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information. [Content from College of the Canyons AB 3720.]**

- Public Records - The California Public Records Act (Government Code Sections 6250 et seq.) includes computer transmissions in the definition of "public record," and nonexempt **electronic** communications made on ~~the College network and computers~~ **any technology medium, College-owned or personal,** must be disclosed if requested by a member of the public. **Refer to AP 3300 Public Records. [Content from College of the Canyons AB 3720. Added reference to Mt. SAC AP 3300.]**

- Litigation - ~~Computer~~ **Electronic** transmissions may be discoverable in litigation.

- **College Rights – The College may access user files or suspend services without notice: 1) to protect the integrity of electronic systems; 2) under time-dependent, critical operational circumstances; 3) as required by and consistent with the law; or 4) when it is reasonable to believe that violations of law or College policy or procedures have occurred. In such cases of access without notice, data or information acquired may be used to initiate or extend an investigation related to the initial cause or as required by law or Board Policy. [Content from College of the Canyons AP 3720.]**

Copyrights and Licenses

~~Computer users~~ **Users** must respect copyrights and licenses ~~to~~ **for** software and other online information.

- Copying - Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any College facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

- ~~Number of Simultaneous Users - The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the~~

~~purchase contract~~. **[Removed 'Number of Simultaneous Users' section that is in the baseline CCLC document.]**

- Copyrights - In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources, including the Internet, must be used in conformance with applicable copyright and other laws. Work deemed protected under Section 107 of the Copyright Act of 1976 ("Fair Use") shall be documented as having satisfied the four-factor test.

Integrity of Information Resources

~~Computer users~~ **Users** must respect the integrity of ~~computer-based information~~ **technology** resources.

- User ID is the Immutable Key – Every user with access to Mt. SAC information resources is assigned a user ID (e.g.**,** jsmith123). This User ID is the immutable key and cannot be changed by IT. A user may update their ~~preferred~~ **chosen** name and display name using the Portal, but the user ID will not be updated or changed. Employees may request an email alias that corresponds with their legal name and/or ~~preferred~~ **chosen** name, with approval from HR and IT, but the user ID used for login will not be updated or changed. **[HR replaced 'preferred' name with 'chosen' name.]**

- Modification or Removal of Equipment - ~~Computer users~~ **Users** must not attempt to modify or remove computer equipment, software, or peripherals ~~that are owned by others~~ without proper authorization **by IT**. **[Removed 'Computer' to focus on user and user access].**

- Unauthorized Use - ~~Computer users~~ **Users** must not interfere with others' access and use of the College ~~computers~~ **technology resources**. This includes, but is not limited to~~:~~**,** the sending of excessive messages, either locally or off-campus; ~~printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known by the user to be available;~~ **using unsupported software applications or hardware;** unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up ~~a~~ College ~~computer or network~~ **electronic resources**; ~~installing or connecting unauthorized equipment;~~ and **disrupting,** damaging**,** or vandalizing College computing facilities, equipment, software, or computer files. **[Updated for clarity. Added unsupported software and hardware.]**

- Unauthorized Programs - ~~Computer users~~ **Users** must not intentionally develop or use programs ~~which~~ **that** disrupt other ~~computer~~ users or ~~which~~ **that** access private or restricted portions of the system, or ~~which~~ **that** damage the software or hardware components of the system. ~~Computer users~~ **Users** must ensure that they do not use programs or utilities that interfere with other ~~computer~~ users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure and may further lead to civil or criminal legal proceedings. **[Removed 'Computer' to focus on user access.]**

- Reporting Problems - Any defects discovered in system operations or system security must be reported promptly to the appropriate system manager so that steps can be taken to investigate and solve the problem. **[Added section on reporting to clarify user responsibility in reporting problems.]**

Usage **[Section reorganized; moved ahead of Unauthorized Access for clarity.]**

The College is a non-profit, tax-exempt organization and, as such, is subject to specific Federal, State, and local laws regarding sources of income, political activities, use of property, and similar matters.

- Unlawful Messages - Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable Federal, State, or other law or College Board Policies or Administrative Procedures, or which constitute the unauthorized release of confidential information. Users shall not send spam, phishing, or other malicious messages. **[Added to address past needs with Student Services hearings regarding a 'student' posting advertising and other misleading information in Canvas.]**

- Commercial Usage - Electronic communication facilities must not be used to transmit commercial or personal advertisements, solicitations, or promotions. College information resources should not be used for commercial purposes. Users are reminded that the ".edu" domain has rules restricting or prohibiting commercial use, and users may not conduct activities not appropriate in the domain.

- User Identification - Users shall not send communications or messages anonymously or without accurately identifying the originating account.

- Political Use - College information resources must not be used for partisan political activities where prohibited by Federal, State, or other applicable laws.

- Prohibition of College Resource Use for Political Campaigning - Employees are prohibited from using College resources, such as email systems, equipment, and supplies, for political campaigning or to support or oppose any ballot measure or candidate in any Federal, State, or Local elections. Users are prohibited from using College resources for Union activities unless specified in the collective bargaining agreements. **[HR added content]**

- Remote Access - Remote access to sensitive College systems is provided based on critical business need. The College reserves the right to audit all remote access client systems and all communications between remote access client systems and the College network for compliance with all applicable security requirements.

- **Information Security Awareness Training - Employees are required to complete Information Security training. This training is to communicate employee responsibilities when working with Controlled Unclassified Information as defined in AP 3721 Information Security.**

Unauthorized Access

~~Computer users~~ **Users** must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

- Abuse of Computing Privileges - Users of College information resources must not access computers, ~~computer~~ software, ~~computer~~ data, ~~or~~ information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the College.

- ~~Reporting Problems - Any defects discovered in system accounting or system security must be reported promptly to the appropriate system manager so that steps can be taken to investigate and solve the problem.~~

- Password Protection - A ~~computer~~ user who has been authorized to use a password-protected account may be ~~subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without authorization of the Chief Technology Officer or designee.~~ **in violation of Board Policies and Administrative Procedures if the user discloses the password or the multi-factor authentication that completes the login requirements for the user or otherwise makes the account available to others.** **[Removed 'account' and 'computer' for clarity. Added MFA section since it is part of authentication. Removed liability section and replaced with violation of College policies and procedures.]**

- **Multi-Factor Authentication - Employees accessing Controlled Unclassified Information electronically will use a supported Multi-Factor Authentication medium as defined in AP 3721 Information Security.** **[Added MFA section and added cross reference to AP3721.]**

~~Usage~~

~~Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of College procedure and may violate applicable law. The College is a non-profit, tax-exempt organization and, as such, is subject to specific Federal, State and local laws regarding sources of income, political activities, use of property, and similar matters.~~

- ~~Unlawful Messages - Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable Federal, State, or other law or College policy, or which constitute the unauthorized release of confidential information.~~

- ~~Commercial Usage - Electronic communication facilities must not be used to transmit commercial or personal advertisements, solicitations, or promotions. Some public discussion groups have been designated for selling items and may be used appropriately, according to the stated purpose of the group(s). College information resources should not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not appropriately within those domains.~~

- ~~Information Belonging to Others - Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.~~

- ~~User Identification and Rights of Individuals - Users shall not send communications or messages anonymously or without accurately identifying the originating account or station. Users must not release any individual's (student, faculty, and staff) personal information to anyone without proper authorization from the individual affected.~~

- ~~Political Use - College information resources must not be used for partisan political activities where prohibited by Federal, State, or other applicable laws.~~

- ~~Personal Use - College information resources should not be used for personal activities not related to appropriate College functions, except in a purely incidental manner so long as: (a) it does not consume more than a trivial amount of system resources; (b) it does not interfere with the productivity of other campus employees; and (c) it does not pre-empt any College activity.~~ **[Redundant. Incidental use was described at top of document.]**

- ~~Captioning/Closed Captioning – All video media posted to the College-affiliated Internet or Intranet must be captioned or sub-titled for the deaf or hard-of-hearing. Any exceptions must be approved by a Human Resources accessibility officer.~~ **[Removed. Closed captioning addressed in AP3450 and AP5142.]**

- ~~Remote Access – Remote access to sensitive College systems is provided by Virtual Private Network (VPN) based on critical business need. VPN access may be requested by completing the VPN request form and obtaining the appropriate approval signatures. Request for VPN access must be approved by the Chief Technology Officer. Mt. SAC reserves the right to audit all VPN client systems and all communications between VPN client systems and Mt. SAC's network for compliance with all applicable security requirements~~. **[Removed VPN access request requirement; statement is a business process.]**

Information Security Awareness Training

Employees ~~with access to sensitive information~~ are required to complete Information Security training. ~~Training must be completed within 30 days of assignment and is mandatory upon hire and annually thereafter.~~ This training is to communicate employee responsibilities when working with Controlled Unclassified Information as defined in AP 3721. ~~The Information~~

~~Security Awareness training program is subject to revision by the Chief Technology Officer or their designee.~~ **[Removed verbiage that is covered in AP3721.]**

~~Multi-Factor Authentication~~

~~Employees accessing sensitive Controlled Unclassified Information digitally will use Multi-Factor Authentication. Multi-Factor Authentication increases account security by requiring a username and password (what you know) and verified access to a registered device (what you have). Multi-Factor Authentication controls are subject to revision by the Chief Technology Officer of their designee.~~

Employee Email Accounts

All ~~Mt. San Antonio~~ College-related email communications must be conducted using ~~an~~ **a College-assigned** email address ~~assigned by the College~~. This restriction is necessary because email originating at the College may contain proprietary information regarding students, staff, or internal College business. ~~The College is responsible for the security of this information and cannot assume that other email providers will provide adequate levels of data backup, security, and virus protection. Therefore,~~ **F**orwarding of email from a Mt. San Antonio College email address ~~to a non Mt. San Antonio College email address~~ is not authorized or allowed. Users may not configure any email program or service to use an automated process for forwarding Mt. San Antonio College email to any other email address. **Email is subject to a three-year retention retention period per AP 3310. Emails in the inbox, sent, draft, junk, and all other folders are permanently deleted and not recoverable.** **[Reference to AP3310 and notation of email data classification plus its transitory nature.]**

~~Student Email Accounts~~

~~Email services are available for students to support learning and for communication by and between the College and themselves. The services are provided only while a student is enrolled in the College. Recognizing that students often pause for a term or intersession and then continue their education at Mt. SAC, student accounts will be discontinued only after a student has not registered for enrollment for four consecutive terms (approximately one year). Once a student is no longer enrolled at the College, access to the account will be removed and the content deleted. If a student re-applies at the College, their email address will be reactivated with an empty mailbox.~~

~~Student email users are advised that electronic data (and communications using the College network for transmission or storage) may be reviewed and/or accessed in accordance with College policy. The College has the authority to access and inspect the contents of any equipment, files, or email on its electronic systems.~~

Student System Access **Accounts**

Systems' use shall not be in violation of State or Federal laws, or in violation of existing Terms of Service agreements with the College's service providers. **[Added to cover use of externally hosted systems and service providers.]**

Student system access, including email services, is available to students, provided it adheres to the guidelines under Integrity of Information Resources and Usage that are not explicitly intended for employees. The services are provided only while a student is enrolled in the College. [Section added to address the need to be an active enrolled student primarily driven by cost prohibitive Google storage costs.]

~~Access to Mt. SAC electronic systems such as the College portal are available for students to support registration and other academic and business services.~~ Recognizing that students often ~~stop out~~ **pause** for a term or intersession and then continue their education at Mt. SAC, student ~~system access~~ **accounts** will be discontinued only after a student has not registered ~~for enrollment~~ for four consecutive terms (approximately one year). Once a student is no longer enrolled at the College, access to ~~College electronic systems~~ **the account** will be removed **and the content deleted**. If a student re-applies at the College, their ~~system access~~ account will be reactivated **and include an empty email box**.

~~Social Media Definition~~

~~Social networking includes networking sites that communicate via the Internet and networking sites that use SMS text or mobile technologies. All genres of social networking sites or media will be referred to below as social media. Currently, popular examples of social media include Facebook, Twitter and similar utilities, sites, and/or resources.~~

~~Social Media Responsibility~~

~~College employees are responsible for the content they post to social media. The College will neither indemnify employees for anything they write on social media nor restrict employee speech on social media not associated with the College. Social media officially affiliated with the College or used by employees to enhance instruction is subject to the following procedures:~~

- ~~College Coursework - Faculty utilizing social media to enhance instruction are responsible as the site administrator for said media.~~

- ~~College Departments - Social media for a College department requires prior approval from the department administrator. An email or written proposal or approval will suffice. Social media for College departments will have a minimum of two site administrators assigned. If a site administrator leaves the College, the department administrator will assign another in their place and the account password will be changed.~~

- ~~College Clubs and Organizations - Social media for College clubs and organizations cannot be affiliated with the College without prior approval from the College club sponsor/advisor or other College employee. Social media for College clubs and organizations should have two site administrators of which at least one is a College employee. Those site administrators can optionally authorize and assign student site administrator(s) and revoke those privileges if the student site administrator(s) is not acting in accordance with these procedures.~~

~~The site administrator(s) shall post their name(s) and a contact method prominently on the site and shall check their pages regularly for prohibited content. Examples of content prohibited from social media officially affiliated with Mt. SAC and, if possible, should be removed by the site administrator upon discovery, are:~~

- ~~derogatory language that can reasonably be interpreted as harassing or threatening any third party;~~

- ~~language or images encouraging or depicting sexual harassment, vandalism, stalking, drinking, drug use, criminal activity, or other behavior prohibited by the Student Standards of Conduct;~~

- ~~content that violates State or Federal law including online gambling and the use (without documented, written permission) of copyrighted material;~~

- ~~information that is obviously libelous; and~~

- ~~pornography or patently obscene material, as defined by law.~~

~~Nondiscrimination~~

~~All users have the right to be free from any conduct connected with the use of the Mt. San Antonio College network and computer resources which discriminates against any person on the basis of Board Policy 3410. No user shall use the College network and computer resources to transmit any message, create any communication of any kind, or store information which violates any College procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.~~ **[Redundant. Removed section that belongs in BP/AP 3410.]**

Dissemination and User Acknowledgment

All users shall be provided with a copy of these Procedures and be directed to familiarize themselves with them.

All employees shall submit a signed agreement to the terms of use outlined in this Administrative Procedure. A notice addressing these procedures shall be presented at the login screen of the College-wide authentication portal. The notice shall appear prior to accessing all portal applications. Accessing College computing resources implies acknowledgement, acceptance, and agreement to these procedures. **[Added for clarity. Removed signature page. Removed signature requirement for students. Specifically requires employees to sign and agree to policy for system access.]**

~~Appendix A: Selected Examples of Unacceptable Use~~

- ~~Revealing passwords to others or allowing someone else to use one's account;~~
- ~~Utilizing network or system ID numbers/names that are not assigned for one's specific use on the designated system;~~
- ~~Attempting to authorize, delete, or alter files or systems not created by oneself without authorization from the Chief Technology Officer or his/her designee;~~
- ~~Not complying with requests from designated personnel to discontinue activities that threaten the integrity of computing resources;~~
- ~~Attempting to defeat data protection schemes or to uncover security vulnerabilities;~~
- ~~Registering a Mt. San Antonio College IP address with any other domain name;~~
- ~~Unauthorized network scanning or attempts to intercept network traffic including the use of unauthorized wireless Access Points or similar devices;~~
- ~~Malicious disruptions such as intentionally introducing a computer virus to the campus network;~~
- ~~Harassing or threatening other users of the campus network; and~~
- ~~Connecting unauthorized equipment directly to the campus network. (Devices such as PDAs, printers, and USB drives that connect to a computer and not directly to the network are acceptable.)~~

[Removed Appendix A for clarity; document focus is acceptable use. References to legacy technologies; removed.]

~~AP 3720 Signature Page: Dissemination and User Acknowledgment~~

~~All users shall be provided copies of AP 3720 and shall be responsible for adhering to its content. Signed agreement is required by all employees to receive system access accounts and utilize the College technology systems and tools.~~

~~The provisions and terms of AP 3720 constitute an agreement between the College and employee as to their agreed-upon rights and duties as such relate to the utilization of the College technology systems and tools. These terms are subject to change only upon mutual written agreement between the College and the respective constituent groups. The College shall make the current version of this document available at http://infosecurity.mtsac.edu. All parties are put on notice that a violation of the above terms and provisions may result in civil, criminal, or other administrative action including the reporting of such activity to the appropriate authorities as required by law, up to and including, but not limited to, loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.~~

~~As an employee of Mt. San Antonio College, I certify that I have read and have received a copy of this Agreement (AP 3720).~~

~~Name: _____~~
~~Print Name~~

~~Name: _____ Date: _____~~
~~Signature~~

[Removed for clarity and focus as an acceptable use document. User agreement statement is in section titled 'Dissemination and User Acknowledgment.']

Revised: March 27, 2013
Reviewed: May 6, 2014
Reviewed: December 16, 2014
Reviewed: June 9, 2015
Reviewed: May 10, 2016
Reviewed: October 2017
Revised: May 25, 2022