Chapter 3 - General Institution

AP 3720 Use of Technology and Information Resources and Employee Acceptable Use Agreement

References:

Education Code Section 70902; 17 U.S.C. § 101 et seq. (Copyright Act); Penal Code Section 502; Academic Senate for California Community Colleges 1999 paper *Academic Freedom, Privacy, Copyright and Fair Use in a Technological World*

The College technology systems 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 are for College instructional and work-related purposes.

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 personal computers, workstations, and associated peripherals, and software and information resources, regardless of whether used for administration, research, teaching, or other purposes.

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.

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).

Users of College technology systems 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.

- Public Records - The California Public Records Act (Government Code Sections 6250 et seq.) includes computer transmissions in the definition of "public record," and nonexempt communications made on the College network and computers must be disclosed if requested by a member of the public.

- Litigation - Computer transmissions may be discoverable in litigation.

Copyrights and Licenses

Computer users must respect copyrights and licenses to software and other on-line 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.

- 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 must respect the integrity of computer-based information 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 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 name, with approval from HR and IT, but the user ID used for login will not be updated or changed.

- Modification or Removal of Equipment - Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

- Unauthorized Use - Computer users must not interfere with others' access and use of the College computers. 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; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a College computer or network; installing or connecting unauthorized equipment; and damaging or vandalizing College computing facilities, equipment, software, or computer files.

- Unauthorized Programs - Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer 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.

Unauthorized Access

Computer 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.

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.

- 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.

- 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.

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.

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 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, forwarding 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.

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

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 for a term or intersession and then continue their education at Mt. SAC, student system access 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 will be removed. If a student re-applies at the College, their system access account will be reactivated.

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.

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.)

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

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