C.01.09.01 Appropriate use of Information Technology Resources Procedure
Responsible Department: VCPPIS
Based on Board Policy: C.01.09 - Appropriate Use of Information Technology Resources
Approved: 8-18-09
Last Amended: 12-15-15; 12-04-23

I. Scope

This procedure applies to all College District information technology resource users, including but not limited to administrators, faculty, students, staff, Board members, agents, volunteers, vendors, and the community, both on campus and at remote sites.

II. Information Technology Resources

College District information technology resources include but are not limited to computer hardware and software including peripheral equipment such as mobile devices, scanners and printers, networking resources, electronic communications such as email, voice mail, internet, intranet, College District and college websites, and all related data and information. These resources are intended for College District business only and are College District property. They are not to be used for employee personal gain or private use (such as non-College District volunteer work), or to advocate for any non-College District related business or purpose.

III. Nondiscrimination

Since College District information technology resources are not unlimited, priority may be given to certain uses or certain groups of users in support of the College District mission. However, the use of information technology resources shall not be denied or abridged because of race, color, religion, gender, national origin, age, genetic information, sexual orientation, disability, veteran or other legally protected status. Requests for accommodations related to the use of information technology resources should be directed to the college disability services department (students) or Human Resources (employees).

IV. No Expectation of Privacy

Users of College District information technology resources have no expectation of privacy regarding information transmitted or received through or stored on College District information technology resources.

V. Appropriate Use

Appropriate use of College District information technology resources includes:

1. Authorized use by students directly related to completion of College District class assignments or other educational pursuits required by the College District,

2. Authorized use by employees directly related to instruction, research, and other College District business in the course and scope of their assigned College District duties. User access to administrative systems is assigned according to a role-based security structure that is applied equally to all employees in a particular College District role.
3. Use by recognized student and campus organizations, and other agencies of the College District directly related to official College District business.

VI. General Standards

General standards are established to provide access to College District information technology resources for official educational and job related purposes of College District students and employees while maintaining the security and integrity of data files and assuring the legal and ethical use of the software.

A. Hardware and Software

1. The College District provides hardware and software as required for employees' particular job functions, to be used only for official College District business. The College District has the sole right to the software and data used and/or stored on such computer equipment. Employees have no claim to such hardware, software or data. Upon termination of employment the College District has no obligation to provide the former employee with copies of any software or data stored on College District computer equipment or systems.
2. No unauthorized software may be loaded on College District computer equipment and no unauthorized computer equipment may be used at College District facilities.
3. Administrative access rights to College District computer equipment shall be determined according to college and College District rules.

B. Internet/Electronic Mail

Access to the Internet and E-mail is College District property and is subject to all requirements regarding use of College District property or equipment.

The use of College District internet access, e-mail, and other communication tools is subject to Public Information Act requirements.

Internet: The Internet is to be used only for accomplishing official College District business by enabling the efficient and timely exchange of information and data. The Internet is made available to employees and students, based on professional and

educational need as determined by the college Presidents or appropriate Vice Chancellor or their designees. Use of the Internet should be guided by common sense and professionalism.

C. ***E-mail and other electronic communication tools*:**

1. E-mail and other electronic communication tools are provided to employees and students to facilitate communication of official College District business to fulfill the College District mission. Electronic communication tools include but are not limited to electronic bulletin boards, information databases, and the ability to forward mail and route documents.
2. E-mail shall be used only for official College District business. College District employees are allocated 2 gigabytes of e-mail storage capacity. E-mail storage capacity over this limit may be administratively deleted.
3. Alamo Colleges will never ask a user to disclose their system credentials or passwords. However, in the event of troubleshooting a user initiated login issue and at the discretion of a supervisor, manager, and/or Alamo Colleges IT support, users may disclose their credentials verbally (never via Email) to confirmed Alamo College's support personnel.
4. All messages transmitted and received via e-mail or instant messaging are subject to the requirements of the Public Information Act. Users are advised to state nothing in an e-mail message that would be inappropriate if published in the news media. All e-mail messages sent or received over College District systems are College District property.
5. No aliases are allowed. All e-mail messages shall be credited to the actual author. All College District employees using E-mail are assigned a unique electronic mailbox, accessible by an employee-controlled password. Employees shall not use another employee's electronic mailbox or password, or attempt to access another employee's or a student's email unless prior consent given by Human Resources, Legal, or Information Technology Services senior administration.
6. No e-mail messages shall be transmitted or stored in encrypted form, unless approved by College District administration.

VII. Security

The College District reserves the right to implement appropriate security measures, including denying access to information technology resources to anyone who, in the opinion of the College District, has misused these resources or does not require access to

certain information and/or systems based on the individual's College District role, as necessary to preserve and maintain system and data integrity. All data transmitted over College District networks and systems is subject to trace or capture.

A. Systems' Security

Users shall comply with College District policies, standards, procedures and rules, and with federal, state, and local laws governing computer and information technology. Abuse of information technology resources is prohibited, including but not limited to:

1. Unauthorized entry or attempted unauthorized entry into a file or system.
2. Unauthorized transfer or attempted unauthorized transfer of a file or other data or information.
3. Allowing unauthorized access to others, either by revealing or not protecting a password, or leaving a computer or terminal without first logging off locking desktop or logging off.
4. Use of another individual's identification or password, or attempting to access another individual's information without appropriate authorization.
5. Use of information technology resources to interfere with the work of an employee or student.
6. Use of information technology resources to access, send, store, or display inappropriate, obscene, harassing or abusive messages or materials.
7. Interference or attempted interference with the normal operation of College District information technology systems.
8. Duplication or use of software or proprietary programs in violation of software licensing agreements.
9. Willful or negligent introduction of computer viruses or disruptive/destructive programs into College District wide-area or local-area networks, or any computer or other component of College District information technology systems.
10. Changing default settings to block remote access by information technologies department administration.

B. Employees' Responsibilities Concerning Security

1. Employees shall not share login credentials.

2. Employees shall report to their immediate supervisor the appearance of mysterious files or login notices which might indicate that the employee's files or systems access has been used without his/her consent.
3. Employees shall not leave an unattended workstation while logged on.
4. Students shall not use employee workstations without appropriate authorization.
5. Employees shall not give system or site-related information to unauthorized persons. Information requests concerning passwords, access, systems design or configurations shall immediately be referred to the supervisor, manager or senior administration.
6. Employees shall not install unauthorized software or download and execute software from the internet or other sources without appropriate authorization and testing.
7. Employees shall not accept instructions to type system-configuration "commands" into a system without appropriate authorization.
8. No e-mail messages shall contain passwords or security related information.
9. Employees shall notify their immediate supervisor, manager, or senior administration, and campus security of any threatening communication received.
10. Employees shall be aware of and comply with restrictions for sharing and disposing of information.
11. Employees shall only connect portable media devices (such as USB drives) that are known to be worm and virus free. It is strongly recommended that a scan be performed on the portable media device using the College District's antivirus software prior to accessing any files on the device. Personal Identifiable Information (PII) information must not be stored on portable media devices.
12. Hacking or unauthorized attempt or entry to Alamo Colleges' information technology Resources is forbidden, and such an action is considered a violation of the Computer Fraud and Abuse Act (CFAA) , 18 U.S.C. § 1030.
13. Staff shall not disable firewall or virus software without the prior consent of the IT Risk & Security office.
14. Alamo Colleges users should be aware the World Wide Web is not censored and may contain some content that some users may find offensive, therefore, Alamo Colleges cannot accept responsibility for what users access, however, if such content is accessed, users must disengage from material immediately.

Note: Records of the College District e-mail system may be public and may be subject to public inspection under the access provision of the Public Information Act. Retention

requirements are based on applicable law and retention schedules, not on the media upon which information is recorded.

VIII. Mobile Devices

Users who utilize Alamo Colleges-owed mobile devices such as laptops, smartphones, tablets and portable storage devices such as USB drives, must take adequate measures to ensure that confidential and/or Personal Identifiable Information (PII) contained in such devices is secure and not available to third parties when taken off-site. Users must employ controls such as encryption and/or passwords to ensure the confidentiality, integrity and availability of such data.

IX. File Transfers and Data Exchanges

Users who wish to transfer files of information must use secure file transfer protocol (SFTP). Requests for all SFTP transfers should be directed to the IT Risk & Security Office for assistance.

X. Cloud Security

Users must only use enterprise-licensed cloud applications approved by Alamo Colleges. Sensitive data such as personal identifiable information (PII) must not be stored in the Cloud without appropriate security measures.

XI. College District Websites

The College District websites, including websites for each college and component, are official publications of the College District and the College District reserves the right to control published content and links. College District websites shall be subject to the same requirements as all other College District publications, including but not limited to, the laws, rules, and regulations regarding copyright, license, and confidentiality of student and employee records. Design and construction of faculty web pages shall be supervised by the appropriate Vice Presidents, Deans, Directors, Department Chairs, or their designees.

The College District webmaster shall have oversight of all College District web page projects.

XII. Licensing

Software is licensed to the College District for specific and restricted use. It is illegal to copy licensed software for personal use, either on campus or off campus. Appropriate authorization must be given to allow licensed software to be installed on an employee's home computer. Pre-approval is required.

XIII. Copyright

All users shall comply with federal copyright laws.

XIV. Inappropriate Use

Using College District information technology resources for purposes other than official College District business is prohibited. Prohibited activities include, but are not limited to:

1. Sending unsolicited electronic mail (such as "spam") that could interfere with College District or other mail servers. Interference with College District electronic communication services includes but is not limited to: misusing mass communication facilities (Listservs, blogs, e-mail distribution lists, propagating "chain letters," virus hoaxes, fraudulent, harassing, or obscene messages (such as threatening, hateful, or racially, ethnically or otherwise offensive); or "bombing" (flooding an individual, group, or system with numerous or large e-mail messages).
2. Using Alamo.edu email, social media and / or listservs to send notices or communications of any kind encouraging or soliciting support for, or opposition to, political and legislative matters when such notices or communications are not directly related to College District business in the course and scope of an employee's assigned College District duties.
3. Communicating non-College District related information on Instant Message Facilities; internal and external Listservs such as DISTALL, SACALL, etc.; and other list-based communications, newsgroups, blogs, Wikis, and social media.
4. Stalking or threatening someone. Using social media, E-mail, chat facilities, blogs, and newsgroups to threaten or stalk someone.
5. Using information technology resources for financial gain or non-College District business. Supporting, establishing, or conducting private business operations or commercial activities, or other non-College District activities, such as volunteer work, or allowing such use by another person or entity.
6. Accessing inappropriate material. Intentionally disseminating, accessing, or providing hyperlinks or access to pornography or obscenity, unless such activities are directly related to an employee's or student's assigned research or completion of an assigned academic requirement.

7. Violating city, state, or federal laws or College District policy or procedures.
8. Defeating system security; for example, "cracking" or guessing and applying the identification or password of another user. Since any account can serve as an entry point for theft, damage or unauthorized use, users shall protect the confidentiality of their personal identification codes and passwords (this provision does not prohibit system administrators and other authorized personnel from using security scan programs within the scope of their authority). Furthermore, users shall not attempt to make any unauthorized changes to data or attempt to intercept or access data or communications intended for another.
9. Misusing IP addresses or other network codes that have been assigned to users as individuals or for use as a College District employee or student. Users shall not seek to obtain unauthorized access to accounts, software, files, or any other College District information technology resources.
10. Attempting to compromise security. College District information technology resources shall not be used in an attempt to compromise the security of College District or any other personal, private, or public information systems.
11. Using excessive network bandwidth. Large-scale distribution of MP3 music, video or other large files can cause excessive network overload. The College District Information Technology Services department reserves the right to manage and restrict any application or practice that involves significant network bandwidth or server load.
12. Establishing unauthorized network or computer connections to or from any of the College District systems or components, including but not limited to the use of remote access software and unauthorized wireless devices or wired network devices.
13. Concealing identity, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading or impersonating others or otherwise using a false identity.
14. Distributing computer viruses. Users shall not knowingly distribute or launch computer viruses, Trojan horses, worms, malware, or other rogue programs.
15. Removing or modifying data, software, or equipment. Without proper authorization, users shall not remove or modify any College District owned or administered equipment or data and may not change any preset or profile

setting including homepages on classroom, lab, or library stations.

16. Modifying system facilities, operating systems, or disk partitions, attempting to crash or hoard College District computer assets or resources. This includes damaging, vandalizing or threatening to damage or vandalize College District information technology resources.
17. Performing illegal functions. Use of information technology resources in violation of civil or criminal laws at the federal, state, or local levels. Examples of such uses are: promoting a pyramid scheme, gambling, distributing obscenity, receiving, transmitting or possessing child pornography, infringing copyrights, or making bomb threats.
18. Violating copyright laws. Copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder under certain conditions for educational purposes. However, an educational purpose does not automatically mean that use is permitted without authorization. For more information on educational copyright applications contact the Vice Chancellor for Academic Success or the Office of Legal Affairs.
19. Violating any software license agreement, including copying or redistributing copyrighted computer software, data, or reports without appropriate written authorization.
20. Unauthorized representation, implying that the user is representing, giving opinions, or otherwise making statements on behalf of the College District or the Information Technology Services department without prior authorization, or using College District trade names, logos, or trademarks without prior written authorization.
21. Intentionally wasting electronic resources or damaging/destroying the integrity of electronic information.
22. Attempting to gain unauthorized access to computers or any other component of College District information technology resources, or using College District information technology resources to attempt to access a system external to the College District.
23. Purposely disrupting the intended use of the Internet, E-mail or other College District information technology resources.
24. Wasting College District resources through activities that cause the employee to be idle or non-productive during work hours. This includes, but is not

limited to, game playing, non-College District related internet surfing (exploring), connecting to non-work related addresses or conducting personal business.

25. Using College District information technology resources negligently or carelessly so as to increase the likelihood that those resources could be damaged, destroyed, or stolen.
26. Knowingly submitting inaccurate or false information for or on any College District record, report, or document.
27. Conduct constituting sexual harassment such as making unwelcome sexual advances, unwelcome requests for sexual favors, or other unwelcome conduct of a sexual nature, or any unwelcome conduct or other offensive unequal treatment of an individual that would not occur but for the gender of the individual (see H.01.02).
28. Transferring, accessing, storing or sending material that is threatening, abusive, pornographic or obscene, or which creates an atmosphere or situation which causes a hostile work or educational environment for an employee or student, regardless of intent.
29. Soliciting funds or services, selling tickets, soliciting for non-College District fund raising, commercial or other activities, or distributing petitions or literature for any purpose other than official College District business.
30. Accessing another employee's e-mail without consent such as unauthorized reading, deleting, copying, modifying or otherwise using any other employee's e-mail without prior permission from Human Resources, Legal, manager or senior administration in response to legal proceedings and/or court order in the preservation or production of evidence.
31. Charitable or commercial advertisements, other than official College District business.

XV. Administrative Access

Users of College District information technology resources have no expectation of privacy regarding information transmitted or received through or stored on College District information technology resources.

In accordance with state and federal law and College District policy and procedures, authorized College District personnel may access College District information technology systems without the consent of the user. Circumstances that warrant such access include but are not limited to:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the information technology systems;
2. When required by federal, state, or local law or College District policy or procedures;
3. When there are reasonable grounds to believe that a violation of law or a breach of College District policy or procedure may have occurred, and access, inspection, or monitoring may produce evidence related to the misconduct;
4. When such access is required to carry out essential College District business functions;
5. When, by attaching privately owned personal computers or other resources to the College District network, users consent to the College District's use of scanning programs for security purposes;
6. When necessary to facilitate recovery from system malfunctions and for other management purposes; or
7. When deemed necessary to preserve public health or safety.

XVI. Enforcement

Failure to adhere to this procedure or Policy C.01.09 or other College District policies related to information technology resources use is grounds for cancellation of access privileges and other disciplinary action. While an investigation is in progress, in order to prevent further possible unauthorized activity, Alamo Colleges senior administration may suspend the authorization of information technology services to the individual or account in question. Whether or not the user is suspected of any violation of these procedures, the Alamo Colleges senior administration may deactivate a user's technology privileges when necessary to preserve the integrity of facilities, user services, or data.

Employees shall promptly report suspected unauthorized use or other violations to the employee's immediate supervisor, a College District administrator, or the college or district services designated security representative. Upon notification, information technology administrators may impose limitations on continued use of technology resources.

Confirmation of unauthorized or fraudulent use of information technology resources may result in disciplinary action, including a student's expulsion, an employee's termination of employment, criminal charges and/or legal action.

XVII. Administration

Knowledge of and administration of these rules is the responsibility of every College District information technology resource user.

XVIII. Review

This procedure and Policy C.01.09 shall be reviewed and updated not less than annually by the Information Technology Leadership Council and the IT Risk & Security officer and submitted to appropriate entities for approval and implementation.

Legal Reference - TACC Policy Reference Manual
CS(LEGAL) - Information Security
DBD(LEGAL) - Employment Requirements and Restrictions: Conflict of Interest