CISCO COLLEGE

Records and Information Privacy

Cisco College complies with the Family Educational Rights and Privacy Act of 1974 (FERPA), as amended, which provides that all students and former students of Cisco College have the right to inspect their educational records (including records, files, documents, and other materials that contain information directly related to students and are maintained by an educational agency or institution or by a person acting for such agency or institution).

Responsibility for protection of the privacy of student educational records rests primarily with the Dean of Enrollment Services. Under the law, at the postsecondary level, parents have no inherent rights to inspect a student's educational records. This right is solely limited to the student. Outlined below are limitations which exist on students' rights to inspect and review their educational records, as published in the Guidelines for Educational Rights and Privacy Act of 1974 as amended, Revised Edition 1995, a publication of the American Association of Collegiate Registrars and Admissions Officers.

Students' Access to Their Educational Records

All students have the right to review their educational records, with the following exceptions as outlined by FERPA:

1. Financial information submitted by parents.

2. Confidential letters and recommendations placed in their files prior to January 1, 1975, provided these letters were collected under established policies of confidentiality and were used only for the purposes for which specifically collected.

3. Confidential letters and statement of recommendation, placed in the records after January 1, 1975, to which the students have waived their right to inspect and review and that are related to the students' admissions, application for employment or job placement, or receipt of honors.

4. Educational records containing information about more than one student; however, in such cases, the institution must permit access to that part of the record which pertains only to the inquiring student

To review records, students and former students may go to the appropriate office of record (e.g., Admissions Office, Financial Aid Office), present a valid photo identification card, and ask to review the record. If it is an inappropriate time to retrieve the record on short notice, students may be requested to complete a "Request to Review Educational Records" form. Because of various circumstances, the College may delay to a maximum of 45 days the release of the records for review. The College is not required to provide access to records of applicants for admission who are denied acceptance or, if accepted, do not attend.

Under the "Family Educational Rights and Privacy Act of 1974," the following is designated as directory information and may be made public, unless the student desires to withhold directory information:

- Student's full name
- Addresses – local, permanent and email
- Telephone listings – local and permanent
- Date of birth
- Major Field of Study
- Participation in officially recognized activities and sports
- Photographs
- Weight and height of members of athletic teams
- Dates of attendance
- Degrees and awards received
- Most recent previous school attended
- Classification
- Enrollment Status.

Students wishing to withhold directory information should complete the appropriate form, available at the Enrollment Services, within 10 days after the first class day. The form is also

available on the College website. Forms received by mail must be accompanied by a copy of a photo ID.

Social Security Number

Section 7(b) of the Privacy Act of 1974 (5 U.S.C. 522a) requires that when any federal, state or local government agency requests an individual to disclose his/her social security account number, the must also be advised whether that disclosure is mandatory or voluntary, by what statutory or other authority the number is solicited and what uses will be made of it. Cisco College will release information under the Audit and Evaluation exception to authorized representatives of the U.S. Comptroller General, the U.S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as a State postsecondary authority that is responsible for supervising Cisco College District's state-supported education programs. Disclosure under this provision may be made, subject to the requirements of §99.35, in connection with an audit or evaluation of Federal or State-supported education programs, or for enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosure of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35).

Accordingly, students or applicants for admission as students are advised that disclosure of a student's social security account number (SSAN) is required as a condition for admission as a student at Cisco College, in view of the practical administrative difficulties which would be encountered in maintaining adequate student records without the continued use of the SSAN.

A randomly generated identification number is issued to each student to be used by students and college personnel in place of the SSAN for accessing student data in the Cisco College administrative system. Cisco College personnel will continue to have access to the student SSAN in the Cisco College administrative system as necessary to verify the identity of the student, and as a student account number (identifier) in order to accurately record necessary data. As an identifier, the SSAN is required for such activities as determining and recording eligibility for admission as a student; determining and recording eligibility for student financial assistance to include loans, scholarships and grants; recording entitlement to and payment of scholarships, grants, allowances; issuing student identification cards; and such other related requirements which may arise.

Authority for requiring the disclosure of a student's SSAN is grounded on Section 7(a)(2) of the Privacy Act, which provides that an agency may continue to require disclosure of an individual's SSAN as a condition for the granting of a right, benefit, or privilege provided by law, where the

agency required this disclosure under statute or regulation prior to January 1, 1975, in order to verify the identity of an individual.

Cisco College has, for several years, consistently required the disclosure of the SSAN on student application forms, and other necessary student forms and documents used pursuant to statutes passed by the State of Texas and the United States, and regulations adopted by the agencies of the State of Texas and the United States, and the Board of Regents

CISCO COLLEGE	
COLLEGE POLICY MANUAL	**POLICY NUMBER:** 3.13
TYPE: Business Operations	**EFFECTIVE DATE:** Immediately
TITLE: Information Resources	**ADOPTION DATE:** March 10, 2008 **REVISION DATE:** July 8, 2019

3.13 INFORMATION RESOURCES

Acceptable Use of State/College-Owned Information Resources

The primary purpose of electronic communication systems at Cisco College is to support and advance the College mission.

Information resources are defined for the purpose of the Acceptable Use Policy as any college-owned computer, video, data communication, or network facilities. The Executive Director of Information Technology Systems with input from the Technology and Distance Learning Advisory Committee will make recommendations for developing Administrative Regulations and Policy for Information Resources.

Purpose

A. To remain competitive, to better serve college constituencies and to provide employees with the best tools to do their work, Cisco College makes available access to electronic media and services, which may include but is not limited to computers, e-mail, databases, software, telephones, voicemail, fax machines, external electronic bulletin boards, wire services, online services, Intranet, Internet and the World Wide Web.

B. Cisco College encourages the use of these media and associated services because they can make communication more efficient and effective and because they are valuable sources of information. However, everyone connected with the college should remember that electronic media and services provided by the college are college property and their purpose is to facilitate and support school business. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

C. To help all employees make responsible decisions, the following guidelines have been established for using information resources. No policy can lay down rules to cover every possible situation. Instead, it is designed to express Cisco College philosophy and set forth general principles when using electronic media and services.

Prohibited Communications

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

1. Discriminatory or harassing;
2. Derogatory to any individual or group;
3. Obscene, sexually explicit or pornographic;
4. Defamatory or threatening;
5. In violation of any license governing the use of software; or
6. Engaged in for any purpose that is illegal or contrary to Cisco College's policy or business interests.
7. For product advertisement or political lobbying

Personal Use

The computers, electronic media and services provided to employees by Cisco College are primarily for work related purposes. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their intended purposes, the employee's job performance or the college budgets. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege. See section four for additional information.

Access to Employee Communications

A. Generally, electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voicemail, telephones, Internet and bulletin board system access, and similar electronic media is not reviewed by the college. However, the following conditions should be noted:

   Cisco College does routinely gather logs for most electronic activities and monitor communications directly, e.g., sites accessed, upload/download content, and time at which transfers are made, for the following purposes:

   1. Cost analysis;
   2. Resource allocation;
   3. Optimum technical management of information resources; and

4. Detecting patterns of use that indicate users are violating college policies or engaging in illegal activity.

B. Cisco College reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other college policies.

C. Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

Software

To prevent computer viruses from being transmitted through the school's computer system, unauthorized downloading of any unauthorized software is strictly prohibited. Only software registered through Cisco College may be downloaded. Employees should contact the Helpdesk if they have any questions.

Security/Appropriate Use

A. Access to Information Technology Resources is granted according to role based needs by appropriate administrators.

B. Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by school administration, employees are prohibited from engaging in, or attempting to engage in:

1. Monitoring or intercepting the files or electronic communications of other employees or third parties;

2. Hacking or obtaining access to systems or accounts they are not authorized to use;

3. Using other people's log-ins or passwords; and

4. Breaching, testing, or monitoring computer or network security measures.

C. No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

D. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

E. Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner. Respect for the intellectual work of others has traditionally been essential to the mission of colleges and universities. We do not tolerate plagiarism, and we do not condone unauthorized copying of software, including programs, applications, databases and code.

F. Appropriate measures will be taken by the IT staff of the college to insure Internet/DATA security. This includes but is not limited to:

1. Insuring SSL standards on all firewalls/routers are kept up to date.

2. Enabling AES-NI Crypto chips on all firewalls.

3. Use of Intrusion Detection on all firewalls.

4. Separating all student network traffic from Staff/Faculty and Student Information System via VLAN.

5. Blocking "Dark Web" sites.

6. Monitoring suspicious IP traffic and blocking if necessary.

7. Port protecting on switches to prevent students from seeing each other on the wifi network.

8. Insuring all of the PC's available for student use in the campus labs are locked down using software (Deep Freeze) so that no information is retained on the computer after the student logs out. Browser settings require display time-out, or sleep mode, after a defined period of inactivity and require user authentication by login to reopen a session.

9. Encryption of all WLAN AP management traffic when deemed necessary to prevent a user from acting as an AP (Access Point).

10. Resetting/changing passwords on a regular basis is encouraged. Staff/Faculty that use the Student Information Service will be forced to change

their passwords every 45 days with minimum standard of at least 8 characters, and alphanumeric mix. This is also applicable to the local domain access.

Participation in Online Forums

A. Employees should remember that any messages or information sent on school-provided facilities to one or more individuals via an electronic network—for example, Internet mailing lists, bulletin boards, and online services—are statements identifiable and attributable to Cisco College.

B. Cisco College recognizes that participation in some forums might be important to the performance of an employee's job function and/or professional responsibilities.

Violations

Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible termination, legal action, and criminal liability.