

Responsibility: Vice President for Financial and Administrative Services
Responsible Executive Officer: President

Source/Reference: [U.S.A. PATRIOT Act of 2001, Public Law 107-56 \(2001\)](#)

PURPOSE

To establish the institution's responsibilities in regard to the requirements of the U.S.A. Patriot Act of 2001 and procedures for responding to requests under the Act.

The [U.S.A. PATRIOT Act of 2001, Public Law 107-56 \(2001\)](#) is designed to broaden the surveillance capabilities of law enforcement agencies in an effort to achieve early detection of potential terrorist plots. Pursuant to the provisions of The Patriot Act and acting under the authority of a valid court order, law enforcement agencies may request various forms of information, records, documents, or data from institutions of higher education. Such data includes, but is not limited to records of borrowed print materials, records of Internet access, e-mail communication records, and telephone usage records. The Patriot Act authorizes law enforcement agencies to install devices to monitor computer access and telephone usage, at the enforcement agency's expense, in libraries and/or information systems departments if necessary to implement the purposes of the Act.

POLICY

- I. Columbia State Community College will respond, as required by the provisions of The Patriot Act, to requests by law enforcement agencies acting under the authority of a valid court order (i.e., warrant or subpoena) by providing to the requesting officials such records, documents or other data that the College maintains.
- II. Records maintained by the College are retained in accordance with state- mandated record retention guidelines. Records shall not be destroyed prior to the date authorized by the retention guidelines, or as a method to avoid compliance with an official request for records.
 - A. Columbia State does not maintain written sign-in logs for computer usage. The College issues each student and employee individual computer identification accounts (log in name and password) for access to the Institution's computer network. The maintenance of accurate computer usage logs occurs electronically through the individual user's log in/log out process. Columbia State informs network users, in its computer use policy, of their responsibility to consistently utilize the log in/log out procedures when accessing the Institution's computer network. Users are also informed that they are responsible for any computer files, databases, and/or Internet sites that are accessed through their computer identification account, notwithstanding their failure to adhere to the log in/log out process, or their voluntary publication of their account information to others. The Teaching and Learning Center and the Library do not maintain records of

individual usage of the computers in areas under the supervision of those departments.

In the event that law enforcement officials request information regarding general computer access of a specific individual, Columbia State shall comply with the request by searching its electronic database of authorized user's log in access to the network.

- B. The provisions of The Patriot Act supercede Tennessee law regarding the confidentiality of library records. Under Tennessee law, a public patron's library records are not public records. Such records are classified as confidential, and library personnel may only disclose the content of those records in certain circumstances permitted by law. Tennessee law permits disclosure of a public patron's library records if: (1) the patron consents; (2) the library must disclose the information to obtain reimbursement for the return of lost or stolen materials; and/or (3) the records requested are pursuant to a court order. In addition to the aforementioned circumstances delineated by state law, The Patriot Act specifies that confidential library records of a patron must be disclosed if a legitimate request for such records from a law enforcement agency is provided as required by the Act. Columbia State does not maintain individual histories of patron usage of printed materials beyond the period of possession (i.e., from check-out to check-in).
- C. Telephone usage records are available only for long distance calls.
- D. The Patriot Act amended certain provisions of the Family Educational Rights and Privacy Act ("FERPA"). Specifically, the amendments grant educational institutions the authority to disclose, without consent or knowledge of the student or parent, personally identifiable information from the student's education records to the Attorney General of the United States or his designee in response to a court order (*ex parte* order from the Attorney General, grand jury subpoena, or law enforcement subpoena) in connection with the investigation or prosecution of terrorism crimes. The amendment to FERPA does not require the Institution to record the disclosure of information from a student's education record when making a disclosure to a law enforcement agency under The Patriot Act.

PROCEDURES

I. Voluntary Reporting of Suspicious Activity

- A. The Patriot Act authorizes voluntary disclosure of the contents of electronic communication to law enforcement officials, if the provider reasonably and objectively believes the institution's computer system has been compromised such that an emergency involving immediate danger of death or serious physical injury may occur without disclosure to a law enforcement agency.

- B. Personnel suspecting a breach of the institution's computer network should discuss the concern with the department's director or dean, providing appropriate documentation or evidence, if available.
- C. The director or dean shall investigate the situation, in consultation with the vice president for financial and administrative services and the associate vice president of information technology.
- D. The vice president for financial and administrative services shall then consult with the president and the Tennessee Board of Regents Office of General Counsel prior to disclosure to law enforcement.
- E. The director of public relations and marketing will be informed immediately following disclosure to a law enforcement official.

II. Response to Requests from Law Enforcement

- A. In any situation in which a law enforcement agency requests previously documented information pursuant to a court order, search warrant, or subpoena, and/or any type of assistance in monitoring information in the future, the individual contacted should immediately notify the vice president for financial and administrative services.
- B. Upon his/her arrival at the institution, the law enforcement officer shall be directed to the vice president for financial and administrative services, who is responsible for directly communicating with officials. In the absence of the vice president for financial and administrative services, the associate vice president for business services shall be responsible for acting on his/her behalf.
- C. If a law enforcement officer presents a court order (i.e., warrant or subpoena), the vice president for financial and administrative services shall do the following:
 - 1. Cooperate with the officer, after verifying that he/she is properly affiliated with a legitimate law enforcement agency and requesting the information for action within the scope of his/her employment with that agency.
 - 2. Contact the TBR Office of General Counsel and decide, in consultation with the Office of General Counsel and the appropriate campus personnel, how best to obtain the records requested.
 - 3. Initiate the process of obtaining the records and delivering them to the requesting official in as expedient manner as possible.
- D. If the law enforcement officer does not provide a court order (i.e., warrant or subpoena) compelling the disclosure of records, the officer should be taken to the vice president for financial and administrative services, who will explain the

confidentiality requirements imposed upon the institution pursuant to its policies, Tennessee Board of Regents policies, and Tennessee and federal laws. (FERPA in the instance of requirements for access to student records.)

E. Confidentiality of Requests

1. All employees involved in the processing of requests for records by law enforcement officials under the provisions of the Patriot Act are required to maintain the confidentiality of such requests.
2. Disclosure of information regarding the request should be limited to the president, the vice president for financial and administrative services, the TBR Office of General Counsel, and other personnel directly involved in responding to the request for records.
3. The TBR Office of General Counsel shall determine the extent of disclosure to other individuals as needed.
4. The vice president for financial and administrative services will maintain accurate, comprehensive, and confidential written documentation of each request for information from law enforcement personnel.
5. The vice president for financial and administrative services will provide copies of the documentation to the president.