LIM College

Effective: 08/01/2012
LIM College - Student

Technology – Federal, State, and Local Laws – LIM College

The IT Department will cooperate fully with any federal, state, or local, law enforcement or other governmental officials investigating the lawful use of LIM College technology resources.

Laws relating to privacy and information technology have become complex. There is no single, comprehensive set of computer use and/or network use laws but there are a few laws specifically applicable to college or university computer use. The Educause Computer and Network Security Task Force published **IT Security for Higher Education: A Legal Perspective** The excerpts below were extracted directly from the **EDUCAUSE Website**: http://www.educause.edu/library/resources/it-security-higher-education-legal-perspective and identified the following laws specifically pertinent to colleges and universities:

Family Education Rights and Privacy Act (FERPA):

FERPA is the keystone federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing "personally identifiable education information," such as grades or financial aid information, without the student's written permission. FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers. While violations of FERPA do not give rise to private rights of action, the U.S. Secretary of Education has established the Family Policy Compliance Office which has the power to investigate and adjudicate FERPA violations and to terminate federal funding to any school that fails to substantially comply with the law.

Please refer to LIM College's FERPA policy, which can be reviewed at: http://www.limcollege.edu/life-at-lim/student-resources/policy-procedures

Electronic Communications Privacy Act (ECPA):

The ECPA has a number of components, but broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. Protection of the "contents" of such communications, however, extends only to information concerning the "substance, purport, or meaning" of the communications. In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved. As a result, the monitoring by institutions of employees' and students' network use or of network usage patterns, generally, would not be prohibited by the ECPA. This statute has both criminal and civil components.

Computer Fraud and Abuse Act (CFAA):

The CFAA criminalizes unauthorized access to a "protected computer" with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer. A "protected computer" is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States. In light of the "interstate or foreign commerce" criterion, the act of "hacking" into a secure web site from an out-of-

state computer may be considered a CFAA violation. This statute has both criminal and civil components.

USA Patriot Act:

The USA PATRIOT Act, grants law enforcement increased access to electronic communications and, among other things, amends FERPA, ECPA and the Foreign Intelligence Surveillance Act of 1978 (FISA), in each case making it easier for law enforcement personnel to gain access to otherwise confidential information. Perhaps most significant in the context of higher education is an amendment that potentially prohibits institutions from revealing the very existence of law enforcement investigations. Under Section 215 of the USA PATRIOT Act, which amends Sections 501 through 503 of FISA, the FBI can, with a court order, seize certain business records pursuant to an investigation of "international terrorism or other clandestine intelligence activities," and record-keepers are prohibited from disclosing the FBI's action to anyone "other than those persons necessary to produce the tangible [records] . . . ." The same goes for investigations into data banks storing information, such as information about who may have accessed certain library resources - thus, librarians may not even reveal that an inquiry has been made.

Digital Millennium Copyright Act (DMCA):

The 1998 enactment of the Digital Millennium Copyright Act (DMCA) represents the most comprehensive reform of United States copyright law in a generation. The DMCA seeks to update U.S. copyright law for the digital age in preparation for ratification of the World Intellectual Property Organization (WIPO) treaties. Key among the topics included in the DMCA are provisions concerning the circumvention of copyright protection systems, fair use in a digital environment, and online service provider (OSP) liability (including details on safe harbors, damages, and "notice and takedown" practices).

Gramm – Leach – Bliley Act (GLBA):

The GLBA34, enacted in 1999, is applicable to financial institutions, including colleges and universities, and creates obligations to protect customer financial information. This includes student financial aid information. The GLBA includes requirements to take steps to ensure the security of personally identifying information of financial institution customers, such as names, addresses, account and credit information, and Social Security numbers. The GLBA also sets forth extensive privacy rules which, among other things, require covered financial institutions to provide customers with privacy statements describing their information privacy practices. However, the Federal Trade Commission's (FTC's) regulations implementing the GLBA specifically provide that colleges and universities will be deemed to be in compliance with the privacy provisions of the GLBA if they are in compliance with FERPA. Nevertheless, educational institutions likely remain subject to the security provisions under the GLBA and the FTC's implementing rules. The GLBA customer financial information security rules, with which institutions must come into compliance by May 23, 2003, will require colleges and universities to develop comprehensive security programs, assess the need for employee training, and include obligations in their agreements with third parties that have access to financial records covered by the rules.

Approved by Senior Cabinet – TBD