



Purpose of the Access and Compliance Form

In 2003, The CSU Chancellor's Office issued a memorandum outlining immediate actions to be taken to tighten existing security measures for those individuals approved to access University protected data. One new CSULA requirement was for all employees accessing campus administrative systems or decentralized systems (i.e., those not managed by ITS) to sign an Access and Compliance form, which is filed in the employee's official personnel file. Only one Access and Compliance form is required per individual and covers all systems that employee may access.

Information Security Training Resources

- FERPA Tutorial – The Family Education Records Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. FERPA certification is mandatory for all employees accessing student information systems. A convenient online tutorial, along with the certificate, is available at: <http://www.calstatela.edu/its/policies/ferpa/>.
- Information Security Training – This online course is sponsored by the Chancellor's Office and provides information on how to protect University information assets, as well as providing valuable information to protect against various risks and threats at work, while traveling, and at home. Request training by sending an e-mail to ITSecurity@calstatela.edu. Requestors will receive a response from *WorkPlace Answers* with instructions and the web link.
- User Guidelines and Standards – Documents on a variety of information technology and information security topics including legal responsibilities and requirements, best practices, and tools/resources are available at <http://www.calstatela.edu/its/policies>.
- IT Security Web Site – This site promotes information security awareness through alerts and advisories, campus information security programs, information security tips, security bulletins, and reference guides.

Access and Compliance Agreement

I certify that I have received training on the state and federal laws, CSU policies, and University guidelines that govern access to and use of information entrusted to CSULA.

I understand that I am being granted access to this information and data based on my agreement to comply with the following terms and conditions:

- I will comply with state and federal laws, CSU policies, and University guidelines that govern access to and use of information accessible through a University information system. While a current summary of state and federal laws is described below, these laws may be revised and that may necessitate additional training requirements.

The California State University (CSU) has responsibility to protect sensitive personal data and maintain confidentiality of that data under the Information Practices ACT (IPA) and Title 5.

The Information Practices Act, California Civil Code §1798, et seq., requires the Chancellor's Office and campuses to collect, use, maintain, and disseminate information relating to individuals in accordance with its provisions. The CSU is obligated under IPA to disclose any breach of system security to California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. CSU General Counsel's records Access Manual located at http://www.calstate.edu/gc/Docs/Records_Access_Manual.doc addresses the IPA disclosure requirements.

Title 5 of the California Code of Regulations, §42396 through §42396.5, address privacy and the principles of personnel information management.

Additional documents on protecting confidential data and links to current state and federal laws are available at <http://www.calstatela.edu/its/policies>.

- My right to access information and/or protected data is strictly limited to the specific information and data that is relevant and necessary for me to perform my job-related duties.
- I will maintain the privacy and confidentiality of the information and protected data that I obtain, including storing and disposing of the information so it remains confidential.
- I will secure access to confidential/ protected data by taking appropriate actions, which may include, but are not limited to, locking the data in cabinets, locking my office, signing off the system when not actively using it, not leaving the protected data open on the computer screen or my desk, etc.
- Before sharing information or protected data with others, electronically or otherwise, I will make reasonable efforts to ensure that the recipient is authorized to receive that information or data. I will sign off the administrative systems or decentralized system prior to leaving the terminal or computer.
- I will keep my password(s) to myself, and will not disclose them to others unless my immediate supervisor authorizes such disclosure in writing.

I understand that if I intentionally misuse personal information or protected data that I obtain through my employment, I may be subject to corrective action (i.e., counseling and reprimands) or disciplinary action (i.e., suspension, discharge, or downgrade) pursuant to the applicable California Education Code provisions and collective bargaining agreements.

I certify that I have read this Access and Compliance form, I understand it, and I agree to comply with its terms and conditions.

Name (please print):

Title:

Signature:

Date: