

### Employee Information That Is Public

The following information concerning CSU employees is a matter of public record and is subject to mandatory disclosure under the California Public Records Act.

Release of this information shall be made available by Human Resources in accordance with government code, section 6250.

Name  
Department/work location  
Funding source  
(Attendance) unit  
County of employment  
Gross salary  
Frequency of pay  
Pay rate  
Shift differential  
Pay period  
Job classification/range  
Time base/FTE  
Dates of appointment and separations

### Employee Information That Is Confidential

The following information concerning CSU employees is personal and must not be disclosed except as permitted under section 1798.24 of the Information Practices Act of 1977. Contact Human Resources for more details.

Social security number  
Number of Tax exemptions  
Amount of Taxes withheld  
Amount of OASDI withheld  
Marital status  
All voluntary/involuntary deduction/reductions (amount and types)  
Survivor's amounts  
Net pay of employee  
Home address  
Home telephone number  
Birth date  
Ethnic data  
Designee for last payroll warrant  
Gender data  
Veteran status  
Performance evaluations  
Disciplines  
Drivers License number  
Credit card number

### California Information Practices Act of 1977

<http://www.privacy.ca.gov/code/ipa.htm>

**Updated CSU memo: Requirements for Protecting Confidential Employee Data**

<http://www.calstate.edu/HRAadm/pdf2005/HR2005-16.pdf>

### Public Records Act

[http://www.leginfo.ca.gov/cgi-](http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270)

[bin/displaycode?section=gov&group=06001-07000&file=6250-6270](http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270)

### Student Directory Information That May Be Disclosed

(FERPA (Section 99.3) and EO 382, California State University, Chico)

### Legitimate Educational Interest

An official or employee of the University may review or access a student's educational record, **without** the student's written permission, in order to perform tasks that are assigned to his /her position or contractual agreement.

### Student Directory Information

The following information may be disclosed without the student's written permission, **unless** the student requests his/her information be restricted. A student may restrict directory information by completing a *Request for Directory Restriction* form in the Student Records and Registration Office (MLIB 180) or through the portal.

Student's full name (including former and other)  
Address and telephone number  
University assigned e-mail address  
Place of birth  
Major field(s) of study  
Degrees and awards received (includes minors and certificates)  
Dates of attendance  
Graduation date and graduation year  
Educational institution most recently attended  
Class level (e.g. sophomore, senior, grad, etc.)  
Participation in officially recognized activities and sports  
Weight and height of members of athletic teams  
Images  
Enrollment status  
- Undergraduate or graduate  
- Full-time or part-time

**ALL OTHER STUDENT DIRECTORY AND ACADEMIC INFORMATION IS NOT RELEASABLE TO THE PUBLIC WITHOUT THE STUDENT'S WRITTEN RELEASE.**

For further questions regarding the release of student information email or call the Registrar's Office at 898-4555

### Family Education and Privacy Act of 1974 (FERPA)

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

### Student Privacy Rights and Student Responsibilities

<http://em.csuchico.edu/sro/ferpa.asp>

### Chico Student Privacy Rights: Executive Memo 01-01

[http://www.csuchico.edu/prs/EMs/EM01/em01\\_01.htm](http://www.csuchico.edu/prs/EMs/EM01/em01_01.htm)

# CSU, Chico Data Confidentiality/ Security Guidelines



# CSU, Chico Confidentiality/Security Guidelines

## Requirements for Handling Confidential Information

In order to safeguard the privacy of employees, efforts must be made to prevent the inadvertent release of information that would constitute an unwarranted invasion of personal privacy.

**University managers/supervisors must establish procedures to assure confidential information is available only to those persons whose work requires access to such information.** This information is not to be released to anyone other than users whose university duties require access. Exceptions can be made by obtaining written permission of the employee whose information is being requested or pursuant to a valid subpoena or other court order.

As a state agency, CSU, Chico is responsible for maintaining employee information in accordance with the Information Practices Act of 1977. Any information that identifies or describes an individual, including statements made by, or attributed to, the individual, is considered confidential and shall not be disseminated without express permission of the individual.

Dissemination to university employees is allowed when the disclosure is relevant and necessary in the ordinary course of the performance of their official duties and is related to the purpose for which the information was acquired.

CSU, Chico is responsible for maintenance, security, and integrity of student academic records and manages student record information in accordance with the Family Rights and Privacy Act of 1974 (also known as FERPA and the Buckley Amendment), and under state, California State University, and local policy based on the requirements of FERPA. FERPA is unambiguous in asserting that the academic and personal information in a student's record may not be released to anyone without the written consent of the student or without legitimate educational interest as determined by the University.

## Guidelines

Employees of CSU, Chico must adhere to the established policy related to the security and confidentiality of employee, student, and financial information. See EM 97-18, Policy on Use of Computing and Communications Technology [http://www.csuchico.edu/prs/Ems/EM97/em97\\_18.htm](http://www.csuchico.edu/prs/Ems/EM97/em97_18.htm). It is each employee's responsibility to maintain employee, student, and financial information in a confidential and secure manner, and to perform his/her job utilizing the best practices security measures stated below:

1. Assure that access to confidential information via university computers or otherwise is used for authorized purposes only. All information processed or obtained is considered to be sensitive and/or confidential. Federal and state laws as well as university policies govern such information. Access to information is based on "need to know" and must be directly related to an employee's assigned duties at the university.
2. Assure the security of whatever information you retrieve or otherwise obtain and provide necessary safeguards to secure all confidential information.
3. Assure that you understand and follow all established procedures governing the reproduction, destruction, or modification of information, before taking that action.
4. Restrict retrieval of information, other computing activities and access, and/or distributions of confidential information to only that information which you have been specifically permitted to access as related to your assigned duties and using only functions and utilities which you have been authorized and trained to use.
5. Only use the information access privileges granted to you for the performance of your job. Never use such access privileges for any personal gain or purpose, or for the personal gain or purpose of family, friends or business affiliates.
6. Your university accounts and passwords are issued for your exclusive use for business purposes and are not to be shared with or delegated to others. You are responsible for the security of your accounts and passwords.
7. Assure that your computer is not left unattended and visible while you are logged on and capable of accessing confidential or sensitive files. If you work in a public area, endeavor to place your monitor so that confidential or sensitive information cannot be seen by those who are not authorized to see it.
8. Assure that printed materials containing confidential information are not left unattended or visible to individuals who are not authorized to have the information.
9. Assure that printed materials containing confidential information are not placed in the wastebasket. Assure the proper disposal of confidential information, i.e., shredding or otherwise disposing of such printed material according to university procedures for the disposal of confidential information.