

Humboldt State University
Information System Access and Compliance Form
for Academic Professionals of California (Unit 4) Employees

Personally identifiable information and other confidential data include, but are not limited to, an individual's Social Security Number (SSN), date of birth (DOB), home address, home telephone number, academic performance record, financial data, physical description, medical history, disciplinary history, gender, ethnicity, and religious preference.

While Humboldt State University employees, consultants, and independent contractors may have exposure to records that contain personally identifiable information and/or other confidential data, they are PROHIBITED from viewing any such data in any University record without written approval in advance by the campus President or Vice President for Administrative Affairs.

SECTION TO BE COMPLETED BY UNIT 4 EMPLOYEE

EMPLOYEE NAME

I certify that I have received the appended state and federal laws and University policies (list also attached) that govern access to and use of information contained in employee, applicant, and student records, including data that is accessible through the Management Information System.

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 the state and federal laws and University policies that govern access to and use of information contained in employee, applicant, and student records, including data that is accessible through the Management Information System. While copies of current state and federal laws are attached, these laws may be revised necessitating additional training and requirements.
- My right to access information and/or 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 data that I obtain, including storing and disposing of the information so it remains confidential.

- I will secure access to confidential/sensitive 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 data open on the computer screen or my desk, etc.
- Before sharing information or 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 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 the normal and reasonable duties of my position require compliance with the above.

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

Employee's Name (print)	Signature	Date
Title	Department	

SECTION TO BE COMPLETED BY DEAN OR DIRECTOR (must be MPP)

My signature below certifies that the above Unit 4 employee is under my general supervision and may require access to personally identifiable information and/or other confidential data about students, faculty, staff, alumni, applicants, patrons, contributors, or other individuals in the performance of his or her job duties.

Dean/Director's Name (print)	Signature	Date

SECTION TO BE COMPLETED BY PRESIDENT OR VICE PRESIDENT FOR ADMINISTRATIVE AFFAIRS

I approve the above Humboldt State University Unit 4 employee being granted access to confidential data in Humboldt State University's records to the extent needed to conduct campus business as required to perform his or her job duties. I reserve the right to revoke this approval at any time should I have reason to believe its continuance could compromise data confidentiality, security, or integrity.

The actual creation of computer log-in accounts for this employee, consultant, or independent contractor to access confidential data requires specific authorization by the appropriate “data owner” as that term is defined in Humboldt State University’s Appropriate Use Policy. The data owner may require additional certifications of agreement and understanding prior to granting such authorization.

Dr. Rollin Richmond, President

Date

OR

Burt Nordstrom, Vice President for Administrative Affairs

Date

**Summaries of Provisions
of the
California Information Practices Act of 1977 and California Penal Code Section 502**

INFORMATION PRACTICES ACT OF 1977

Article 10. Penalties

1798.55 – The intentional violation of any provision of this chapter or any rules or regulations adopted thereunder, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment.

1798.56 – Any person who willfully requests or obtains any record containing personal or confidential information from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than five thousand dollars (\$5,000), or imprisoned not more than one year, or both.

CALIFORNIA PENAL CODE SECTION 502

Section 502 is intended to provide protection to individuals, businesses, and governmental agencies such as Humboldt State University from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.

502 Computer crimes – Status as felonies:

- (b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense.
- (c) Any person who maliciously accesses, alters, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.
- (d) Any person who violates the provisions of subdivision (b) or (c) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

– End of Summaries –

ADDITIONAL INFORMATION SOURCES

Further information on applicable state and federal laws can be obtained at the following Web site locations:

- Information Practices Act of 1977
<http://www.privacy.ca.gov/code/ipa.htm>
- California Code of Regulations – Title V
<http://ccr.oal.ca.gov>
- Family Educational Rights and Privacy Act (FERPA)
<http://www.ed.gov/offices/OM/fpco/ferpa/>
- CSU Coded Memorandum HR2002-27 – Requirements for Protecting Confidential Data
<http://www.calstate.edu/HRAAdm/pdf2002/HR2002-27.pdf>
- CSU Coded Memorandum HR2003-5 – Requirements for Protecting Confidential Data - Updated
<http://www.calstate.edu/HRAAdm/pdf2003/HR2003-5.pdf>
- CSU Records Access Manual (February 2003)
http://www.calstate.edu/Gc/Docs/Records_Access_Manual.doc

HUMBOLDT STATE UNIVERSITY APPROPRIATE USE POLICY

The Humboldt State University Appropriate Use Policy is available on the Humboldt State University Web site at

<http://www.humboldt.edu/~its/planning/policy/aup.html>