CSUN

California State University, Northridge

Confidentiality Statement for Consultants, and Independent Contractors Accessing University Data

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.

CSUN consultants, and independent contractors are **prohibited** from viewing CSUN records that contain personally identifiable information and/or other confidential data without written approval in advance by the Vice President for Administration and Finance.

SECTION TO BE COMPLETED BY Consultant or Independent Contractor

I certify that I have read and understand the attached "Summaries of the California Information Practices Act of 1977 and California Penal Code Section 502."

I certify that, in order to ensure the privacy and security of data, I agree to:

- Access, distribute, share, and retain confidential data only as authorized and only as needed to conduct campus business as required to perform my job duties
- Store under secure conditions all confidential data that I retain and ensure its confidential and timely destruction when no longer needed to conduct campus business as required by my job
- Respect the confidentiality and privacy of individuals whose data I access
- Observe any ethical restrictions that apply to data to which I have access
- Protect confidential information located on my workstation.
- Report immediately to my supervisor any and all apparent and suspected information security breaches
- Comply with all CSUN information security policies

I certify that I agree NOT to:

- Discuss verbally or distribute in electronic or printed formats any confidential data except as authorized and as needed to conduct campus business as required to perform my job duties
- Make unauthorized copies of confidential data
- Knowingly falsely identify myself
- Gain or attempt to gain unauthorized access to confidential data or University computing systems
- Share my user ID(s) and password(s) with anyone nor use anyone else's user ID(s) or password(s), except as authorized
- Leave my workstation unattended and unsecured while logged-in to University computing systems
- Use or allow other persons to use University data for personal gain
- Engage in any activity that could compromise the security or confidentiality of data held in University records

I certify that I have read this Confidentiality Statement, I understand it and I agree to comply with its terms and conditions.

Name (Please Print): _____

Signature: _____

Date: _____

Department/Company: _____

Title: _____

CSUN ID#: _____

Email address: _____

Phone number: _____

SECTION TO BE COMPLETED BY CSUN Department Manager

My signature below certifies that the above consultant, or independent contractor, who is under my supervision, 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.

Name (Please Print): _____

Signature: _____

Date: _____

Email address: _____

Phone number: _____

SECTION TO BE COMPLETED BY Vice President for Administration and Finance

My signature below certifies that the above consultant, or independent contractor, who is under supervision by the above CSUN Department Manager, 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.

Name (Please Print): _____

Signature: _____

Date: _____

ADDITIONAL INFORMATION SOURCES

Further information on applicable state and federal laws can be obtained at the following web sites:

- Information Privacy Act (https://www.hhs.gov/foia/privacy/index.html)
- FERPA (http://www.ed.gov/offices/OM/fpco/ferpa/)
- CSU Policies and Standards (http://www.calstate.edu/icsuam/documents/Section8000.pdf)
- CSU Records Retention (http://calstate.edu/recordsretention)
- CSUN Acceptable Use Policy (http://www.csun.edu/sites/default/files/500-10.pdf)
- CSUN Policies and Procedures (http://www.csun.edu/afvp/university-policies-procedures)
- California Penal Code 502 (https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=502.&lawCode=PEN)

Summaries 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 CSUN from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.

c) Any person who commits any of the following acts is guilty of a public offense: (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data. (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network. (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section. (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. (11) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.

d) 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.

e) Any person who violates any of the provisions of paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision (c) is guilty of a felony, punishable by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years and a fine not exceeding ten thousand dollars ($10,000), or a misdemeanor, punishable by imprisonment in a county jail not exceeding one year, by a fine not exceeding five thousand dollars ($5,000), or by both that fine and imprisonment.

End of Summaries