



**SAN JOSÉ STATE
UNIVERSITY**

Office of the President

Jon Whitmore, President

One Washington Square
San José, California 95192-0002
Office: 408-924-1177
Fax: 408-924-1199
sjsupres@sjsu.edu

www.sjsu.edu

November 19, 2008

To: Heads, Chairs, Deans, Directors and Vice Presidents
From: Jon Whitmore, President

Subject: Presidential Directive 2008-03

**Institutional Policy on Access and Control of Information
Contained in Employee Records**

The purpose of this Presidential Directive is to ensure that San José State University continues to comply with all Federal and State legislation and California State University policies regarding the access and control of information contained in employee records. For background information on the development of this policy, please see Presidential Directive 2008-02, Institutional Policy on Access and Control of Information Contained in Student Records.

This Presidential Directive originally was issued on August 25, 2008. The current revised version was reissued on November 19, 2008, and includes section **1.1.2 Research Use** that was inadvertently omitted from the original version.

San José State University
Institutional Policy on Access and Control of Information Contained in Employee Records

Institutional policy for the access and control of information contained in employee records operates in compliance with state and federal statutes, including, but not limited to, the California Information Practices Act (IPA) and the California Public Records Act (PRA). The IPA, PRA and other state and federal statutes protects information maintained by the University that identifies or describes an individual (personal information), including, but not limited to, name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history. In order to assess the right of a person or entity to obtain timely and efficient availability of institutional data reports for all users, an Institutional Data Management Council (IDMC), appointed by the President, is in charge of the development of institutional policies and operational guidelines for the management and delivery of such data.

The policy is based on the following principles:

1. **Accuracy:** Accuracy of data is the responsibility of all members of the university community, even though accountability is assigned to particular units and individuals.
2. **Responsiveness:** The university is committed to the principle of continuous improvement in its responsiveness in providing institutional data.
3. **Limited Redundancy:** Since duplication of data increases the likelihood of data inaccuracy and effort, the university will strive to reduce excessive redundancy in its data and systems.
4. **Security:** The university is committed to securing confidential data while providing reasonable access to authorized users.

RELEASE OF INFORMATION FOR THE PUBLIC

Beyond disclosure that is required and/or permitted by the IPA or PRA no individual data are provided to the general public, including individuals, businesses, or organizations. Requests for an exception to release individual employee data from public individuals or organizations may come to IDMC with university senior administrators as the requestor.

INFORMATION FOR USE WITHIN SAN JOSE STATE UNIVERSITY

1. Requesting Individual Employee Data

To obtain data, including, but not limited to personal information, from individual employee records, a request must be submitted in writing. Approved requests will be assigned to the appropriate university office(s) for response. Release of Social Security numbers is not permitted. Medical records are excluded as part of this policy per CSU HIPAA Privacy Policy located at http://www.calstate.edu/Benefits/pdf/CSU_HIPAA_Policy.pdf. Requests for individual employee data are evaluated and granted on a case by case basis by the Associate Vice President for Human Resources.

All employee data are released for internal use by the requestor only, except as defined in section 1.1.2, Research Use. The requestor, and specified designees, must agree to use any released data only for the purposes specified in the request and must agree that released data will not be reproduced, published, publicly posted, or used for any secondary purpose. The requestor also agrees that he or she will destroy any data with personal information once he or she no longer has a legitimate business use for the information in the ordinary course of his or her official responsibilities. Misuse of any such data may subject requestors or their designees to civil or criminal penalties and/or University discipline.

Any dispute regarding a request for release of individual employee data may be submitted to the IDMC for resolution using a petition for hearing.

1.1. Individual Employee Data Access Privileges and Procedures

The authorization process and type of employee data that may be provided varies according to the administrative responsibilities of the requestor. Requests for employee data are evaluated and approved for the following purposes:

1.1.1. SJSU Administrative Use

Authorization to submit a request for release of individual employee data must first be approved or denied by the appropriate area senior administrator. Requests must demonstrate a legitimate business interest and must be relevant and necessary in the ordinary course of the performance of the official administrative responsibilities of the sponsoring individual, department or organization (hereafter referred to as the requestor).

1.1.2. Research Use

With appropriate approval, all individual employee data may be provided to researchers affiliated with SJSU, or working in conjunction with SJSU faculty or management personnel. The requestor must submit proof of SJSU Institutional Review Board (IRB) approval when making a request for any employee data to be used in scholarly research. If the requestor is a matriculated student, the request must be authorized by the researcher's faculty advisor at SJSU, by the faculty advisor's department chair or director, and by the college dean of the sponsoring department at SJSU. In instances where the sponsoring department does not report to a college dean, the request must be authorized by the appropriate senior administrator for that unit.

In evaluating requests from researchers for surveys of employees, the IDMC and other units as appropriate will work collaboratively to determine the institutional impact of surveying employees, e.g., to ensure that employees are not asked to participate in an inappropriately high number of surveys. Requests for employee contact data from researchers wishing to survey employees may be approved or denied.

2. Requesting Aggregate Data

Aggregate data is defined as data that are compiled or computed, and that exclude any record-level values of any nature, including but not limited to personal identifying information such as names and/or SJSU Identification numbers (EMPLID). Requests for aggregate employee data are evaluated on a case by case basis. Submitted requests are approved or denied by the Associate Vice President for Human Resources and/or the Office of Institutional Research.

Requests from recognized external organizations such governmental entities are reviewed by the AVP of HR and/or the Office of Institutional Research and may be referred to IDMC for further review as appropriate.

3. Use of Employee Data for Mass E-mail Service

Requests for the university's use of mass e-mail service are evaluated on a case-by-case basis and are approved or denied by senior administrators of the Office of Public Affairs within the Division of University Advancement who will notify the University Computing and Telecommunication (UCAT) for processing. Only university email addresses will be used.

Requests must demonstrate a legitimate business interest and must be relevant to the administrative responsibilities of the sponsoring department or organization. The Public Affairs Office reserve the right to edit and format e-mails according to university publications standards. The requesting department must provide an SJSU e-mail address where recipients may send replies and where returned e-mail is sent. The requesting department assumes responsibility for replies and returned e-mail. No attachments can be accommodated. Additional information must be posted on a separate website with appropriate link provided in the e-mail.