

SOCIAL SECURITY NUMBER PROCEDURES AND GUIDELINES

June 2005

PURPOSE

California State University, Chico recognizes that it collects and maintains confidential information relating to its students, employees, and individuals associated with the University and is dedicated to the privacy and proper handling of this information. The primary purpose of this document is to ensure that the necessary procedures, guidelines and awareness exists to provide compliance with both the letter and the spirit of the Family Educational Rights and Privacy Act, the Privacy Act of 1974, the Information Practices Act of 1977 and other legislation regarding the use of social security numbers. The University is guided by the following objectives:

- Broad awareness of the confidential nature of the social security number;
- Reduced reliance upon the social security number for identification purposes;
- A consistent set of procedures addressing the treatment of social security numbers throughout the University; and
- Increased confidence by students and employees that social security numbers are handled in a confidential manner.

PROCEDURES AND GUIDELINES

California State University, Chico is working to minimize the use of social security numbers within its business processes. The social security number will not be disclosed to individuals or agencies outside the university except as allowed by law or with permission from the individual. The Information Security Office, in conjunction with campus Data Custodians, has responsibility for overseeing social security number usage. The Chief Information Security Officer (CISO) will control the social security number and his/her approval will be required to use the social security number in any new campus computing system.

Chico State ID Number

- A university wide Chico State ID will be assigned to all students, employees, and other associated individuals, such as contractors or consultants for use with university business. (PS EMPLID)
- The Chico State ID will be assigned at the earliest possible point of contact between the individual and the University.
- The Chico State ID will be used in all future campus electronic and paper data systems to identify, track, and service individuals associated with the University except where the University is legally required to collect a social security number. It will be permanently and uniquely associated with the individual to whom it is originally assigned.
- The Chico State ID will be considered the property of California State University, Chico and its use and governance shall be at the discretion of the University, within the parameters of the law.

- All services rendered by California State University, Chico and electronic business systems will rely on the identification and authentication services provided by the Chico State ID except where the University is legally required to use a social security number.
- The Chico State ID will not be considered directory information in the student's academic record, but will be treated as sensitive information.

Social Security Number

- The social security number will be treated as confidential information and will never be publicly posted or displayed in any manner.
- The last four digits of the social security number shall be treated the same as the entire social security number.
- The social security number will be electronically transmitted only through encrypted mechanisms except where the University is legally required to transmit to another agency and an encrypted mechanism is not allowed or provided.
- The social security number will be stored encrypted if the means to encrypt is allowable, available, and practicable.
- All University forms and documents shall be modified to collect the Chico State ID, rather than the social security number. Forms and documents will be modified on an *as reprinted* basis with full compliance by fall 2006.
- Paper and electronic documents containing social security numbers will be disposed of in a *secure fashion* (e.g. shredding or otherwise disposing of printed material according to university procedures, CDs and other non-rewritable media should either be broken or defaced by scratching before disposal, deleting electronic data using appropriate university approved utilities, etc.).
- Except where the University is legally required to collect a social security number, individuals will not be required to provide their social security number, verbally or in writing, at any *point of service*, nor will they be denied access to those services should they refuse to provide a social security number. However, individuals may volunteer their social security number if they wish as an alternate means of locating a record.
- These procedures and guidelines do not preclude, if a primary means of identification is unavailable, California State University employees from using the social security number as needed during the execution of their duties. The other aspects of these procedures and guidelines bind such usage.
- Social security numbers will only be collected in circumstances where the collection is mandated by a government agency.

The social security number may continue to be stored as a confidential attribute associated with an individual. The social security number will be used as

1. Allowed by law;
2. A key to identify individuals for whom a Chico State ID is not known.

Social security numbers will be released by the University to entities outside the University only

1. As allowed by law; **OR**
2. When permission is granted by the individual; **OR**
3. When the external entity is acting as the University's contractor or agent and adequate security measures are in place to prevent unauthorized dissemination to third parties; **OR**
4. When CSU General Counsel has approved the release.

The Information Security Office will maintain the list of approved entities.

IMPLEMENTATION

The Information Security Office will have the responsibility to:

- Oversee and ensure the implementation of these procedures and guidelines;
- Provide support, guidance, and problem resolution for offices working with social security numbers;
- Serve as an intermediary between campus units and CSU General Counsel when an opinion on the release or exchange of social security numbers is required;
- Maintain a list of entities, approved by CSU General Counsel, to which social security numbers may be released;
- Produce an educational program to train employees on the handling of social security numbers and make students aware of their rights and responsibilities with regard to social security numbers;
- Ensure uniformity in implementation details, and an adherence to the spirit of these procedures and guidelines;
- Authorize the use of social security numbers in new electronic computing systems.

Information Resources (IRES) will, as part of its data management strategy, develop a set of guidelines addressing the handling of social security numbers in electronic systems. Adherence to these guidelines in all future development will be considered a requirement. These guidelines will explicitly address:

- The display of social security numbers on computer terminals, screens, and reports;
- The security protocol required to access social security numbers when they are included in part of an electronic database;
- Alternate mechanisms for integrating data other than the use of social security number;
- The legal requirement to maintain confidentiality of the social security numbers imposed by FERPA and the California Information Practices Act;
- Obtaining permission to include the Social Security number in a system.

California State University, Chico will adopt a *phased compliance strategy* with the goal of attaining complete compliance with these procedures and guidelines within two years.

Phased Compliance Strategy Timetable

- Phase I generally consists of approving these procedures and guidelines and broadly educating University employees about social security number collection and usage; Completion March 2006
- Phase II prioritizes systems and services out of compliance, and begins remediation or replacing systems; Completion July 2006
- Phase III completes remediation or replacement of systems out of compliance, and monitors and supports existing or developing systems and procedures. Completion June 2007