

POLICIES AND PROCEDURES

Subject: **Protecting the Security and Confidentiality of
Social Security Numbers**

Policy No. **14**

Pages: **7**

Date: **July 1, 2009**

Approved by: Maria M. Houser, Associate Vice President for Human Resources/Labor Relations

Signature:

POLICY

It is the policy of SCSU to protect the confidential nature of Social Security numbers without creating unjustified barriers to the conduct of the business of the University and the provision of services to its many constituencies. Nothing in this policy is intended to prohibit or restrict the collection, use, and maintenance of Social Security numbers as required by applicable law.

SCOPE

This policy applies to all University employees including part-time, temporary and student workers. All employees and associates of the University are to protect the security and confidentiality of Social Security numbers held by the University for business or legal purposes and to comply with Federal and Connecticut law.

Definitions

Breach – shall mean unauthorized access to or acquisition of documents, electronic files, media, data or computerized data containing personal information. This includes events when (1) the access to the personal information has been compromised; (2) the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; or (3) the encryption of personal information has been decoded.

Personal Information – shall mean information capable of being associated with a particular individual through one or more identifiers, including but not limited to, a Social Security Number (SSN), a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number. It does not include publicly available information that is lawfully made available to

the general public from federal, state or local government records or widely distributed media.

User – is any person, whether authorized or not, who makes any use of any IT System from any location. For example, Users include a person who accesses IT Systems in a University computer cluster, or via an electronic network.

Collection, Use, and Disclosure of Social Security Numbers

The University shall collect Social Security numbers from individuals only when legally required to do so or when essential for the conduct of University business. Access to Social Security numbers collected for these purposes shall be limited to those employees who require such access in connection with their job duties. University employees may not disclose Social Security numbers they have obtained from University records, except when legally permitted and essential for the conduct of University business.

Security of Social Security Numbers

Paper records containing a Social Security number must be stored in locked drawers, filing cabinets, or storage rooms and may not be left unattended while in use. Paper records containing a Social Security number may not be removed from the University offices where they are used, unless University business requires they be transferred to another secure office. Unencrypted electronic records containing a Social Security number may be stored only on University servers that meet the highest security standard maintained by the Office of Information Technology. Electronic records containing a Social Security number may be stored on other electronic devices only if the records or the storage drives are encrypted.

Any University employee who learns that a record containing a Social Security number has been lost or stolen or has been subject to unauthorized access must report the incident to the Chief Information Officer as well as the Associate Vice President of Human Resources and Labor Relations.

Remediation of Existing Records Containing Social Security Numbers

University employees are responsible for identifying records in their possession that contain a Social Security number. Whenever such records are identified;

- the records must be stored in compliance with this Policy; or
- the Social Security numbers must be removed or masked; or
- the records must be shredded or electronically destroyed.

Social Security Numbers in Archival Material

University **personnel files and student records** held in archives may contain Social Security numbers. Such records will be held in a secure storage facility. Any records authorized by University officials to be viewed by individuals other than the owner of the record will first be reviewed and the Social Security numbers will be masked or removed to the extent it is reasonably possible to do so.

Other University **administrative records** held in archives may also contain Social Security numbers. Such records will be held in a secure storage facility and will not be available to unauthorized individuals. If authorized, such records will be reviewed and Social Security numbers will be masked or removed to the extent it is reasonably possible to do so.

PROCEDURES

A. Reducing the Use and Collection of Social Security Numbers

- The use of the Social Security number as an individual's primary identification number will be discontinued unless required by law. Social Security numbers may continue to be stored as a confidential feature associated with an individual.
- When permitted by law, Social Security numbers will be collected and used only as reasonably necessary for the proper administration or accomplishment of the University's business, governmental, educational and medical purposes. Reasonably necessary uses include, but are not limited to:
 1. As a means of identifying an individual for whom an alternative identification number is not known; and
 2. For internal verification or administrative purposes.
- Except where permitted by law, individuals will not be required to provide their Social Security number and will not be denied access to services if they refuse to disclose their Social Security number. Individuals may always volunteer their Social Security number as an alternate means of locating a record or accessing services.

Questions about whether a particular use is required by law should be directed to the Chief Information Officer or the Human Resources Office.

B. Informing Individuals When the University Collects Social Security Numbers

Requests for Social Security numbers must include the notice required by Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 552a) and Connecticut Public Act 08-167 effective 10/01/2008. The following statement is available on the SCSU Human Resources web site.

SCSU Privacy Protection Policy for Social Security Numbers

This Policy is publicly posted in compliance with Connecticut Public Act 08-167, which became effective on October 1, 2008.

SCSU may collect certain personal information, including Social Security numbers, in the course of our business. Social Security numbers are routinely collected by SCSU from the University's own employees, as well as from other individuals who perform services for us. We will make what we believe to be reasonable efforts to protect the confidentiality of the Social Security numbers we collect. We protect the confidentiality of the Social Security numbers we collect in the course of our business by maintaining physical, electronic and procedural safeguards to prevent access to this information by anyone who does not have a legitimate need to receive or review it. These safeguards include:

- Limiting access to the Social Security numbers we collect
- Prohibiting unlawful disclosure of the Social Security numbers we collect
- Reviewing these safeguards on a periodic basis
- Training our employees in the proper handling of Social Security numbers

Last Update: 22-June-2009

While it is preferable for notices to be provided in writing, if circumstances require that the notices be provided in an alternate manner, the written notices should be delivered to assure that the notices are properly and consistently given.

Oral presentations of notices (for visually impaired) or Braille notices (hearing impaired) must be documented in writing, noting the date, the name of the person to whom the notices were given and the name of the person providing the notices. The documentation should be maintained by the department providing the notification.

C. Reducing the Public Display of Social Security Numbers

- Grades may not be publicly posted or displayed in a manner in which all or any portion of a Social Security number identifies the individual associated with the information.
- Social Security numbers may not be displayed on documents that can be widely seen by the general public (such as time cards, rosters, and bulletin board postings) unless required by law. This section does not prohibit the inclusion of a Social Security number on transcripts or on materials for Federal or State data reporting requirements
- When documents containing Social Security numbers are sent through the mail, reasonable steps must be taken to place the Social Security number on the document so as not to reveal the number in the envelope window. As an alternative, the Social Security number field may be left blank and the individual may be requested to complete and return the document, if the proper notices are included on the request.
- Employees are prohibited from sending Social Security numbers over the Internet or by email unless the connection is secure or the Social Security number is encrypted or otherwise secured. Employees sending Social Security numbers by fax are required to take appropriate measures to protect the confidentiality of the fax, such as confirming with the recipient that the recipient is monitoring the fax machine.
- The University will comply with all applicable provisions of Public Act No. 08-167 *"An Act concerning the Confidentiality of Social Security Numbers"* and any other legislation, statute or regulation applying to the privacy of Social Security numbers.

D. Controlling Access to Social Security Numbers

- Only those employees who need to see a Social Security number for the performance of their job responsibilities may access records containing Social Security numbers.

- Deans and Department Heads will monitor access to records containing Social Security numbers by the use of appropriate measures as determined by the University.
- Deans and Department Heads will protect the security of records containing Social Security numbers during storage using physical and technical safeguards such as encrypting electronic records, including backups, and locking rooms or cabinets containing physical files.
- Records containing Social Security numbers may not be stored on institutional or personal computers or other electronic devices that are not secured against unauthorized access.
- Social Security numbers may not be shared with third parties except:
 - a. As required or permitted by law; or
 - b. With the consent of the individual; or
 - c. Where the third party is the agent or contractor for the University and appropriate safeguards are in place to prevent unauthorized distribution; or
 - d. As approved by the Associate VP of HR and Labor Relations

Rules of Conduct

- An employee who fails to comply with the rules of conduct may be subject to appropriate disciplinary action, including termination in accordance with the University's policies and procedures.
- Employees may not ask for a Social Security number if it is not necessary and relevant to the purposes of the University and the particular function for which the employee is responsible.
- Employees may not disclose Social Security numbers to unauthorized persons or entities
- Employees who are responsible for the maintenance of records that contain Social Security numbers shall observe all administrative, technical and physical safeguards established by the University in order to protect the confidentiality of such records
- Employees shall promptly report to their supervisors any inappropriate disclosure of Social Security numbers; the supervisor is responsible for reporting the disclosure to the Associate Vice President of Human Resources and Labor Relations. An employee may make a report anonymously if he or she so chooses. Retaliation against an employee who, in good faith, reports a possibly inappropriate disclosure of Social Security numbers is prohibited.

Disciplinary Procedures

Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures as outlined in the Connecticut General Statutes, the State Personnel Act, the Human Resources Policies for Management and Confidential Professional Personnel and other applicable University policies. Staff members who are members of University-recognized bargaining units will be disciplined for violations of this Policy in accordance with the relevant disciplinary provisions set forth in the agreements covering their bargaining units.

Violators may also face Office of Information Technology-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges.

Legal Liability for Unlawful Use

In addition to University discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

AUTHORITY

- Federal Privacy Act of 1974 (Section 7 of Pub. L. 93-579 in Historical Note), 5 U. S. C., § 552a
- Social Security Act, 42 U. S. C. §§ 408(a)(8) and 405(c)(2)(C)(viii)(I)
- CT Public Act No. 08-167 “An Act concerning the Confidentiality of Social Security Numbers” (Effective October 1, 2008)
- The Federal Education Records and Privacy Act of 1974 (FERPA)
- Conn. Gen. Stat. § 42-470
- Conn. Gen. Stat. § 36a-701b
- Health Insurance Portability and Accountability Act (HIPAA)
- Social Security Act, 42 U. S. C. §§ 408(a)(8) and 405(c)(2)(C)(viii)(I)
- Family Educational Rights and Privacy Act, 20 U. S. C. § 1232g
- National Archives and Records Administration General Records Schedule
- Connecticut State Library General Letter 2009-1 “Transfer of Records to the State Archives”
- CT State Library – “Records Retention Schedules for State Agencies”
- CSU Board of Trustees “Resolution concerning Collection, Storage, Use and Disclosure of Social Security Numbers” (BR #02-31)

Exceptions

Any exceptions to this policy shall require prior written approval from the Associate Vice President of Human Resources and Labor Relations or designee.