NOTE: THIS POLICY IS BEING REVISED. THE CHIEF INFORMATION SECURITY OFFICER IS NOW RESPONSIBLE FOR SSN CONFIDENTIALITY.

I. PURPOSE

This policy establishes requirements and guidelines for the protection of the confidentiality of social security numbers.

II. POLICY

It is the policy of The University of Texas at Dallas to protect the confidential nature of social security numbers without creating unjustified obstacles 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.

III. PROCEDURES

A Reducing the Use and Collection of Social Security Numbers

1. The use of the social security number as an individual's primary identification number will be discontinued by September 1, 2007, unless required by law. Social security numbers may continue to be stored as a confidential attribute associated with an individual.

2. 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:

a. As a means of identifying an individual for whom an alternative identification number is not known; and

b. For internal verification or administrative purposes.

3. Except where permitted by law, individuals will not be required to provide their social security number, nor will they 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 University SSN Coordinator.

B. Informing Individuals When the University Collects Social Security Numbers.

1. 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).

2. When a social security number is collected by means of a form completed and filed by the individual, whether the form is printed or electronic, the individual must be provided the notice required by Section 559.003 of the Texas Government Code.

3. Notices will use language approved by the University SSN Coordinator.

4. While it is preferable for notices to be provided in writing, if circumstances require that the notices be provided orally, the written notices should be read to assure that the notices are properly and consistently given. Oral presentations of notices must be documented in writing, noting the date, the name of the person to whom the notices were read and the name of the person providing the oral notices. The documentation should be maintained by the department providing the oral notification for review by the SSN Coordinator and/or internal auditors.

C. Reducing the Public Display of Social Security Numbers

1. Grades may not be publicly posted or displayed in a manner in which all or any portion of either a social security number or an alternative identifier identifies the individual associated with the information.

2. 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

3. 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.

4. 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.

5. The University will comply with any applicable provisions of the Texas Government Code, the Texas Education Code, the Texas Business and Commerce Code, and any other legislation, statute or regulation applying to the privacy of Social Security Numbers.

D. Controlling Access to Social Security Numbers

1. 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.

2. Deans and department heads will monitor access to records containing social security numbers by the use of appropriate measures as determined by the University.

3. 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.

4. 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.

5. 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 Office of General Counsel.

6. When social security numbers are shared with a third party that is the agent or contractor for the University, a written agreement will be executed to protect the confidentiality of the social security number as required by System BPM 66.

E. Protecting Social Security Number with Security Safeguards

1. The University has implemented the following plan, known as the **Social Security Number Record Security Plan,** for records and record systems that contain Social Security Numbers.

a. The Social Security Number Record Security Plan describes the University's safeguards to protect records and record systems containing Social Security Numbers.

b. Administrative Safeguards. The University has addressed the administrative aspects of Social Security Number record security by the adoption of this policy.

c. Physical Safeguards. The University has addressed the physical security of record and record systems containing SSNs by limiting access to such records to only those employees who have a business reason to access the SSNs. Paper documents containing SSNs are kept in file cabinets, rooms or vaults which are locked each night. Only authorized employees know combinations and/or the location of keys. Paper documents that contain SSNs are shredded at the time of disposal.

d. Technical Safeguards. The University has addressed the technical security of electronic records and record systems by the adoption of the Information Resources Use and Security Policy, A5-110.0. This policy addresses acceptable use, e-mail, incident management, privacy, passwords, physical access, security and server hardening, and other issues related to the technical safety of electronic records and record systems. The relevant portions of the Information Resources Use and Security Policy, and any related electronic records security policies, are hereby incorporated into this policy by reference.

2. Employees are required to secure records containing social security numbers in accordance with Section E.1. of this policy.

3. Records or media (such as disks, tapes, hard drives) containing social security numbers will be discarded:

a. In a way that protects the confidentiality of the social security number, such as shredding, reformatting, erasing, or otherwise modifying the material to make it unreadable or indecipherable; and

b. In accordance with the University's records retention schedule.

4. Information systems acquired or developed after January 30, 2004 must comply with System BPM 66. Information systems in the process of being acquired or development on January 30, 2004 are exempt from these requirements:

F. Establishing Accountability for Protecting the Confidentiality of Social Security Numbers

1. Employees will be trained on compliance with this policy and System BPM 66. Training will be in accordance with the following schedule:

a. New employees within 30 days after their initial date of employment; and

b. All employees once every two years.

2. Employees with access to social security numbers will acknowledge their awareness of the provisions of this policy, System Business Procedures Memorandum 66 and other related policies and procedures, by such means as are compatible with the training described in Section III.F.1. above.

3. The University will include social security number confidentiality in institutional risk assessments and related audits.

4. The President is responsible for compliance with this policy, and has designated the Director of Human Resources to serve as the University's SSN Coordinator.

5. Employees are required to report the inappropriate disclosure of social security numbers in a prompt manner. The report may be made by contacting their supervisor, the University SSN Coordinator, or by calling the compliance hotline at 1-888-228-7707. Retaliation against an employee who in good faith reports an inappropriate disclosure of social security numbers is prohibited. If the supervisor and SSN Coordinator determine that social security numbers were inappropriately disclosed and individuals have been put at risk of identity theft or other harm as a result of the disclosure, the University will take all reasonable steps to promptly notify the individuals affected.

6. The university has adopted the following rules of conduct applicable to employees and students. A person who fails to comply with these rules may be subject to appropriate disciplinary action, including discharge or dismissal in accordance with the University's policies and procedures.

a. Employees and students will comply with the provisions of this policy and all related policies and procedures;

b. Employees may not request disclosure of 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;

c. Employees and students may not disclose social security numbers to unauthorized persons or entities;

d. Employees and students may not seek out or use social security numbers relating to others for their own interest or advantage; and

e. Employees responsible for the maintenance of records containing social security numbers will observe all institutionally-established administrative, technical, and physical safeguards in order to protect the confidentiality of such records.

IV. DEFINITIONS

Employee: Both full-time and part-time positions at the university, whether the position is filled or to be filled by a regular or temporary worker, and including student workers and faculty.

Student: A person (a) currently enrolled at the university, or (b) accepted for admission or readmission to the university, or (c) enrolled at the university in a prior semester or summer session and eligible to continue enrollment in the semester or summer session that immediately follows.

V. AUTHORITY

The statutory authority for this policy is provided by Texas Education Code § 65.31. General Powers and Duties. This policy is intended to comply with the following laws:

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)
Family Educational Rights and Privacy Act, 20 U. S. C. § 1232g
Texas Business and Commerce Code, § 35.58, as added by 78th Leg., SB 611
Texas Government Code, § 559.003

VI. INTERPRETATION

The University SSN Coordinator is responsible for interpreting and revising this policy as necessary to meet the changing needs of the University and statutory requirements. For more information, contact the UTD SSN Coordinator.