Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Protecting Confidentiality of Social Security Numbers**
Regulation and Procedure Number:	**URP: 01.275**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

The purpose of this policy is to provide information and rules for protecting the confidential nature of social security numbers used at or by the University, without creating unreasonable obstacles to the conduct of business at the University.

APPLICABILITY

This policy is applicable to TWU Students, Faculty, and Employees.

DEFINITIONS

None

REGULATION AND PROCEDURE

I. Policy

A. It is the policy of Texas Woman's University 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 the policy is intended to prohibit or restrict the collection, use and maintenance of social security numbers as required by applicable law.

B. Social security number is not to be used as an individual's primary identification number, unless applicable law requires such to be used. The social security number may continue to be stored as a confidential attribute associated with an individual.

C. Except in those instances in which collection of a social security number is legally required, an individual will not be required to provide his or her social security number, nor will the individual be denied access to the services at

issue if the individual refuses to disclose his or her social security number. An individual, however, may volunteer his or her social security number as an alternate means of locating a record or accessing services.

II. Collection Use and Disclosure

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 will be limited to those employees who require such access in connection with their job duties. University employees may not disclose Social Security numbers that they have obtained from University records, except when legally permitted and essential for the conduct of University business.

III. Security of Social Security Numbers

A. Employees who are responsible for the maintenance of records that contain social security numbers will observe all administrative, technical and physical safeguards established by the University in order to protect the confidentiality of such records.

1. 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.

2. Paper records containing a Social Security number may not be removed from the University offices where they are used, unless University business requires that they be transferred to another secure office.

B. Social security numbers may not be shared with third parties except as required by law, with the consent of the individual, or when a third party is an agent or contractor for the University. As of September 1, 2005, when social security numbers are shared with a third party, a written agreement should be entered into between the University and the third party. The written agreement should:

1. Prohibit the third party from disclosing social security numbers, except as required by law.

2. Require the third party to use adequate administrative, physical and technical safeguards to protect the confidentiality of records containing social security numbers.

3. Require the third party to be held accountable for compliance with the written agreement through regular monitoring.

C. Employees may not send social security numbers or other confidential information over a fax, the internet or by e-mail unless the connection is secure or the confidential information is encrypted or otherwise secured. Records containing social security numbers or other confidential information should not be stored on University or personal computers or other electronic devices that are not secured against unauthorized access.

1. Unencrypted electronic records containing a Social Security number may be stored only on University servers that meet the highest security standard maintained by Information Technology Solutions.

2. Electronic records containing a Social Security number may be stored on other electronic devices only if the records or the storage drives are encrypted.

3. Records or media (such as disks, tapes, hard drives, flash drives) that contain social security numbers will be discarded in a way that protects the confidentiality of the social security numbers and in accordance with the University's records retention schedule.

IV. Reporting Inappropriate Disclosures, Losses or Thefts of Social Security Numbers

A. Employees will promptly report to their supervisors any inappropriate disclosure, loss or theft of social security numbers. The supervisor is responsible for reporting the disclosure, loss or theft to the computer security officer, if appropriate, the Vice President for Finance and Administration and the responsible Vice President.

B. An employee may make a report anonymously, if he or she so chooses.

C. Retaliation against an employee who, in good faith, reports a possibly inappropriate disclosure of social security numbers is prohibited.

D. 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 Vice President of Finance and Administration as soon as practical.

V. 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 until they reach the appropriate and legal time for disposal

VI. Disciplinary Procedures

Employees will comply with the provisions of this and other related University policies and procedures. An employee who fails to comply with the following may be subject to appropriate disciplinary action, up to and including termination in accordance with the University's policies, procedures and guidelines.

REVIEW

This policy will remain in effect and published until it is reviewed, updated, or archived. This policy is to be reviewed once every six years. Interim review may be required as a result of updates to federal and state law or regulations, Board of Regents policies, or internal processes or procedures.

REFERENCES

None

FORMS AND TOOLS

None

Publication Date:

Next Review: