UTEP Standard 13: Control and Protection of Social Security Numbers

This Standard is established by The University of Texas at El Paso (UTEP) for the proper solicitation and use of Social Security Numbers (SSNs) as reasonably necessary in carrying out its responsibilities and conducting its daily business and academic activities that support its mission. Accordingly, the requirements of this Standard apply to all or part of a social security number in any medium, including paper records, which are collected, maintained, used, or disclosed by UTEP. This Standard applies to all individuals, including students, retirees, employees, and external constituents.

13.1 UTEP shall discontinue the use of all or part of the Social Security Number as an individual's primary identification number unless required or permitted by law. The Social Security Number may be stored as a Confidential attribute associated with an individual only if use of the number is essential for the performance of a mission related duty.

(a) The University shall not utilize all or part of an individual's Social Security Number unless required or permitted by Federal or State law. SSNs shall not be used as the primary identifier for basic campus services, unless required by statute. The SSN may be stored as a confidential attribute associated with an individual only if use of the SSN is essential for the performance of a mission related duty.

(b) If the maintenance and use of social security numbers is permitted, but not required by applicable law, the Institution shall permit the maintenance and use of social security numbers only as reasonably necessary for the proper administration or accomplishment of their respective business, governmental, educational and medical purposes and only if the Institution determines that the necessity outweighs the potential Risk created by the particular maintenance or use of the social security number. Potential purpose may include:

i. use as a means of identifying an individual for whom a unique identification number is not known;

ii. use for internal verification or administrative purposes where it is not feasible to use some other identifier; and

iii. use for verification or administrative purposes by a third-part or its agent in conducting UTEP's business on behalf of UTEP where the third-part or agent has contracted to comply with the safeguards described in UTEP Standard 11: Safeguarding Data.

(b) Except in those instances in which UTEP is legally required to collect a social security number, an individual shall not be required to disclose all or part of his or her social security number, nor shall

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. UTEP's request that an individual provide his or her social security number for verification of the individual's identity where the social security number has already been disclosed does not constitute a disclosure of purposes of this Standard. The notice shall use the applicable text from preapproved sample disclosures or such other text as may be approved by the CISO who will consult with the Office of Legal Affairs with respect to the interpretation of law. Questions should be directed to the Information Security Office.

(c) UTEP may, but is not required to, designate only selected offices and positions as authorized to request that an individual disclose his or her social security number.

(d) UTEP shall assign a unique identifier (e.g., UTEP 80/88 or 600) for each applicant, student, employee, insured dependent, research subject, patient, alumnus, donor, contractor, retiree, and other individuals, as applicable, at the earliest possible point of contact between the individual and UTEP for use in lieu of a Social Security Number.

(e) The unique identifier shall be used in all electronic and paper Information Systems to identify, track, and serve these individuals. The unique identifier shall:

i. be a component of a system that provides a mechanism for the public identification of individuals;

ii. be permanent and unique within the Institution as applicable, and remain the property of, and subject to the rules of, that Institution; and

iii. not be derived from the social security number of the individual; or, in the alternative, if the unique identifier is derived from the Social Security Number, it must be computationally infeasible to ascertain the social security number from the corresponding unique identifier.

(f) All services and Information Systems shall rely on the identification services provided by the unique identifier system.

13.2 UTEP shall provide notice to individuals when they collect Social Security Numbers.

(a) Each time the University requests that an individual initially disclose his or her social security number, it shall provide the notice required by Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 552a), which requires that the individual be informed whether the disclosure is mandatory or voluntary, by what statutory or other authority the number is solicited, and what uses will be made of it. A subsequent request for production of a social security number for verification purposes does not require the provision of another notice.

i. The notice shall use the applicable text from Preapproved Sample Disclosures or such other text as may be approved by the Office of Legal Affairs or Office of General Counsel.

ii. Notices shall be in writing if possible. If a verbal notice is required, such notice shall be promptly documented.

(b) In addition to the notice required by the Federal Privacy Act, when the social security number is collected by means of a form completed and filed by the individual, whether the form is printed or electronic, the notice as required by Section 559.003 of the Texas Government Code must also be provided. That section requires that the agency state on the paper form or prominently post on the Internet site in connection with the form that: with few exceptions, the individual is entitled on request to be informed about the Information that is collected about the individual; under Sections 552.021 and 552.023 of the Government Code, the individual is entitled to receive and review the Information; and under Section 559.004 of the Government Code, the individual is entitled to have the incorrect Information about the individual corrected.

(c) Employees and/or retirees may not seek out or use social security numbers relating to others for their own interest or advantage.

(d) The University shall eliminate the public display of social security numbers.

i. Grades may not be publicly posted or displayed in a manner in which all or any portion of either the social security number or the unique identifier identifies the individual associated with the Information.

ii. Social security numbers shall not be displayed on documents that are accessible to individuals who do not have a business reason to access the numbers. This section does not prohibit the inclusion of the social security number

on transcripts or on materials for Federal or State Data reporting requirements.

iii. If the University must send materials containing social security numbers through the mail, the social security number must be placed in an envelope in such a way that ensures that no part of the social security number is visible from the outside.

iv. The University prohibits employees and/or retirees 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. The University shall require employees and/or retirees -sending social security numbers by fax to take appropriate measures to protect the confidentiality of the fax (such measures may include confirming with the recipient that the recipient is monitoring the fax machine).

v. The University shall not print or permit a third-party acting on behalf of UTEP to require that an individual's social security number be printed on a card or other device required to access a product or service provided by, on behalf of, or through the University.

13.3 All Information Systems acquired or developed must comply with the following:

(a) the Information System must use the social security number only as a Data element or alternate key to a database and not as a primary key to a database;

(b) the Information System must not display social security numbers visually (such as on monitors, printed forms, system outputs) unless required or permitted by law or permitted by this Standard;

(c) name and directory systems must be capable of being indexed or keyed on the unique identifier, once it is assigned, and not on the social security number; and

(d) for those databases that require social security numbers, the databases may automatically cross-reference between the social security number and other Information through the use of conversion tables within the Information System or other technical mechanisms.

13.4 Disposal of documents (e.g., paper, electronic, etc.) containing SSNs, provided state retention requirements have been met, will be disposed of in a secure fashion, such as shredding. Computer files containing SSNs residing on disks, tapes, hard drives, USBs, etc. must be destroyed appropriately and in accordance with the UTEP Electronic Data Destruction Guidelines

13.5 Storage of documents containing SSNs in paper, computerized or electronic documents, or files shall be protected at all times using physical and technical safeguards.

(a) Computer or electronic files containing SSNs shall not be stored or reside on equipment or systems that are not protected against unauthorized access. Users shall store documents or other media containing SSNs or other information essential to the mission of the University on centrally managed servers rather than a local hard drive or portable device. In cases when a user must create or store SSNs on a local hard drive or portable device such as a laptop, computer, tablet computer, smart phone, etc., the user must ensure that the data is encrypted and that the device abides by all University and UTS System standards and policies.

(b) Specific permission must be obtained from the Department Head, Chair or Dean AND the CISO before a user may store SSNs on any personally owned computers, mobile devices, USB thumb drives, or similar devices. Such permission should be granted only upon demonstration of a business need and an assessment of the risk introduced by the possibility of unauthorized access or loss of the data. Any personally owned computing device that contains SSNs must be encrypted and configured to comply with all required University and UT System security controls as well as all policies and standards while holding such data.

(c) Users who store SSNs using commercial cloud services must use services provided or sanctioned by the University rather than personally obtained cloud services.

(d) Physical files containing SSNs shall be secured and made available only to authorized staff.

13.6 Employees shall promptly report inappropriate disclosure or use of SSNs to their supervisors, who shall report the disclosure to the Information Security Office.

13.7 Related Policies, Standards, Procedures, Guidelines and Applicable Laws

- UTEP Information Resources Use and Security Policy
- Standard 2: Acceptable Use of Information Resources
- Standard 11: Safeguarding Data
- UTEP Minimum Security Standards for Systems

- VPBA Records Retention, Destruction and Storage
- UTS 115 Records and Information Management
- UT System UTS-165
- Texas Administrative Code 202
- Government Code, Title 5 Subtitle A, Chapter 559
- Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 552a)

13.8 Revision History

Revised:	February 6, 2008
Revised:	January 28, 2010 (revised and moved to ISO website)
Approved:	May 5, 2017 Gerard D. Cochrane Jr., Chief Information Security Officer
Revised:	June 20, 2019 (addition of retirees; fix broken links; remove UTS preapproved sample disclosure statements-no longer published; 13.5 (a)-(c) clarify what is/is not allowed with regards to storage of documents/media containing SSNs)
Approved:	June 20, 2019 Gerard D. Cochrane Jr., Chief Information Security Officer