5.8.21 Data Classification

Chapter 5 - Information Technology	Original Effective Date: October 2004
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: December 2019

I. Purpose

To establish a standard and procedure for identifying critical data.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. UT Health San Antonio shall establish an Institutional Data Classification Standard that conforms to or maps to the U.T. System Data Classification Standard defined in UTS 165 Standard 9.5. The Data Classification Standard consists of mutually exclusive data classifications based on fit within a spectrum indicating the degree to which access to the data must be restricted and data integrity and availability must be preserved.

The Chief Information Security Officer must develop a plan for identifying digital data maintained in both Centralized and Decentralized IT.

Owners of Information Resources must classify data based on UT Health San Antonio's Data Classification Standard.

B. Classification Standards

1. Confidential/High Risk: Information or data is classified as Confidential if it must be protected from unauthorized disclosure or public release based on state or federal law or regulation, and by applicable legal agreement to the extent permitted by law. Data types include:

a. Protected Health Information: clinical patient records, identifiable patient research records.

b. Student Identifiable Information: student demographic information, performance, financial, or health records, etc.

c. Personnel Information: institutional and departmental personnel records that contain private information on an employee.

d. Sensitive Digital Research Data: Electronic data requiring highest levels of protection due to the following circumstances:

   i. data collected is subject to protection under federal or state law (HIPAA, FERPA, social security numbers);

   ii. data received or collected must be protected under specific requirements of externally-supported research agreements;

   iii. the project under which the data is being collected carries a security classification established by an authorized agency of the federal government;

   iv. information or data collected would violate the confidentiality of sources or subjects involved in the research; and,

   v. other instances where data collected warrants additional protection; designation of data subject to this circumstance will be made by the Vice President for Research.

e. Other Sensitive Information: Other information that presents a significant competitive or regulatory disclosure risk including, but not limited to, intellectual property subject to a confidentiality obligation, Homeland Security information, Social Security Numbers, information described in University of Texas System Policy UTS 165, "Information Resources Use and Security Policy", data related to University Police and Internal Audit investigations, and data that describes University network and computing configurations and security controls.

2. Controlled: The Controlled classification applies to information or data that is not generally created for or made available for public consumption but may be subject to release to the public through request via the Texas Public Information Act or similar State or Federal law. Data types include:

   a. Operational records, operational statistics, employee salaries, budgets, expenditures.

   b. Internal communications that do not contain Confidential Information.

   c. Research Data that has not yet been published, but which does not contain Confidential Information protected by law.

3. Published: Published information or data includes all data made available to the public through posting to public websites, distribution through email, social media, print publications or other media outlets. Data types include:
    a. Statistical reports, Fast Facts, published research, unrestricted directory information, educational content available to the public at no cost.

C. Credit Card Data

1. Credit Card Data (Cardholder Data) that is stored, processed or transmitted shall be classified as Confidential/High Risk and with Policy, Standards and Procedures defined and documented to secure Confidential data.
    a. Cardholder Data is defined as follows:
    b. Primary Account Number (PAN)
    c. Cardholder name
    d. Expiration date
    e. Service code
    f. Full track data (magnetic stripe data or equivalent on a chip)
    g. CAV2/CVC2/CVV2/CID
    h. Personal Identification Numbers (PINs)/PIN blocks
2. Information Resource Owners and Custodians shall notify the Chief Information Security Officer of new and modified Information Resources that store, process or transmit Cardholder Data.

D. Social Security Numbers

1. UT Health San Antonio shall adopt and document Policies, Standards and Procedures that conform to UT System Use and Protection of Social Security Numbers Standard defined in UTS165 Standard 13.
2. 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);
    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.

3. Information Resource Owners and Custodians shall notify the Chief Information Security Officer of new and modified Information Resources that store, process or transmit social security numbers.

E. Accountability

Violations of this policy are subject to disciplinary action as described in the Handbook of Operating Policies (HOP), Section 2.1.2, "Handbook of Operating Policies".

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

UT System (UTS) Policy
UTS 165 Information Resources Use and Security, Standard 9: Data Classification
UTS 165 Information Resources Use and Security, Standard 13: Use and Protection of Social Security Numbers

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a timeperiod that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
10/2004	Policy Origination		
10/2016	Policy Revision		
12/2019	Policy Review		
02/2023	Policy Review/Discretionary Edits		