UTSA Institutional Compliance
Office of Information Security

OIS 10 – Standard for Data Encryption

I. STANDARD STATEMENT

Data encryption is a process of securing computer files by instituting safeguards that make the files unreadable to everyone except for the holder of the encryption key. Data encryption is required on all laptops owned by UTSA.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. Encrypting UTSA-owned/leased desktops
   1. All high risk desktop computers owned, leased, or controlled by the university must be passphrase protected and encrypted using methods approved by the Information Security Officer.
   2. All desktop computers purchased after September 1, 2013 must be passphrase protected and encrypted using methods approved by the Information Security Officer before their deployment.

B. Encrypting UTSA laptop computers and other mobile devices.
   1. All laptop computers and other mobile devices, including but not limited to mobile and smart phones, and tablet computers that are owned, leased, or controlled by the university, must be encrypted using methods approved by the Information Security Officer.
   2. USB thumb drives and similar removable storage devices owned, leased, or controlled by the university must be encrypted before storage of any confidential university data on the device.

C. What is "Sensitive Data"?

The UTSA Office of Information Security has developed the Data Classification Standard to help you determine the sensitivity of your data. While whole disk encryption is required for UTSA owned laptops and desktops, encryption and passwords are recommended for all portable devices to ensure data is secure.

D. Encryption for Personally-owned Computers

1. A personally owned computer must be encrypted if it contains any of the following types of university information.
   a. Information made confidential by federal or state law, regulation, or other legal agreement. This includes, but is not limited to, data protected by FERPA, HIPAA, the Texas Public Information Act, and the Texas breach reporting law (Business &Commerce Code Section 521.002(a)(2)).
      Examples: education records, patient medical treatment and payment records, Social Security Numbers, credit card numbers.
   b. Federal, state, university, or privately sponsored research that requires confidentiality or is deemed sensitive by the funding entity.
   c. Any other information which has been deemed by the UT System or a UT System institution as essential to the mission or operations of System to the extent that its integrity and security should be maintained at all times.

E. "University information" refers to all recorded information created or received by or on behalf of the university (or System) that documents activities in the conduct of state business or the use of public resources. This includes all information generated by a university employee in the course of performing his or her duties regardless of whether it was created and/or located on a personal device owned by the employee.

Title: OIS 10 – Standard for Data Encryption
Effective Date: January 1, 2014
Last Revised: July 30, 2020