UTSA Institutional Compliance
Office of Information Security

OIS 30 – Standard for Portable Computing Security

I. STANDARD STATEMENT

The UTSA Standard for Portable Computing Security establishes guidance for the use of mobile computing devices - such as laptops, tablets and smartphones and their connection to the network - to preserve the integrity, availability and confidentiality of UTSA information.

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. The UTSA Standard for Portable Computing applies equally to all individuals who use portable computing devices and access UTSA information resources.

B. Laptops

1. Laptops must be protected by a password or other authentication device/process.
2. Category I UTSA data should not be stored on laptops.
3. All UTSA-owned laptops must be encrypted using industry-accepted/approved encryption techniques.
4. All remote access to UTSA should occur through the UTSA Virtual Private Network (VPN).
5. User-owned laptops that are used to access the UTSA computer network must conform to UTSA Information Resource Standards and have antivirus/anti-malware software installed.

6. Unattended portable computing devices must be physically secured. They must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

C. Other Mobile Devices

1. Mobile devices such as smartphones or tablets often contain private data such as contact information, passwords, phone numbers and store/financial account log in information. UTSA Category I data should not be stored on any mobile device.

2. Where possible, users must
   a. Install antivirus/anti-malware software
   b. Set a Personally-Identifiable Number (PIN) or password/passphrase
   c. Turn on data encryption (may require use of a password)
   d. Install apps from trusted sources only
   e. Install a locator app or turn on the native locator app
   f. Turn off unneeded services
   g. Uninstall unused applications

Title: OIS 30 – Standard for Portable Computing Security
Effective Date: May 31, 2011
Last Revised: August 4, 2020