# I. 5.8.32 Prohibited Technology Security

| | |
|---|---|
| Chapter 5 - Information Technology | Original Effective Date: December 2024 |
| Section: 5.8 Information Security | Date Last Reviewed: |
| Responsible Entity: Chief Information Security Officer | Date Last Revised: |

## II. Purpose

To establish standards and processes to protect Information Resources owned by UT Health San Antonio and to comply with the Statewide Plan for Prohibited Technologies published by the Texas Department of Public Safety (DPS) and Department of Information Resources (DIR).

## III. 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.

## IV. Policy

A. UT Health San Antonio-Owned Devices

1. Except where approved exceptions apply, the use or download of prohibited applications or websites is prohibited on all UT Health San Antonio-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.
2. The Chief Information Security Officer in coordination with the UT Health IT Department must identify, track, and control UT Health San Antonio-owned devices to prohibit the installation of or access to all prohibited applications.
3. The Chief Information Security Officer in coordination with the UT Health IT Department must manage all UT Health San Antonio-issued mobile devices by implementing the following minimum security controls:
    a. Restrict access to prohibit the installation of Prohibited Technologies;
    b. Maintain the ability to remotely wipe non-compliant or compromised mobile devices;

c. Maintain the ability to remotely uninstall Prohibited Technologies from mobile devices; and

d. Deploy secure baseline configurations for mobile devices, as determined by UT Health San Antonio.

4. The Chief Information Officer in coordination with the UT Health IT Department, must implement the removal and prohibition of Prohibited Technologies, including any future additions to the published list.

B. Personal Devices Used for State Business

Employees and contractors may not install or operate Prohibited Technologies on any personal device that is used to conduct UT Health San Antonio business.

C. Identification of Sensitive Locations

1. UT Health San Antonio must identify, catalog, and label Sensitive Locations. A sensitive location is any location, physical, or logical with specific compliance requirements mandating limited access, such as a Sensitive Compartmentalized Information Facility (SCIF) and controlled technology facility (data center and equipment installed in a main distribution frame and independent distribution frame).

2. Information Resource owners shall identify the information resources under their control that requires protection from unauthorized disclosure that will only be discussed or accessible within Sensitive Locations.

3. Devices containing Prohibited Technology must not enter or access Sensitive Locations.

4. Visitors granted access to Sensitive Locations are subject to the same limitations on Prohibited Technology-enabled devices when entering or accessing secure locations.

D. Network Restrictions

1. The Chief Information Security Officer in coordination with the UT Health IT Department will configure network and device security to prevent access to and from Prohibited Technologies on UT Health San Antonio's technology infrastructure.

2. The Chief Information Security Officer will prohibit personal devices with Prohibited Technologies from connecting to UT Health San Antonio's technology infrastructure.

3. The Chief Information Security Officer in coordination with the UT Health IT Department may provide a wholly separate network for access to Prohibited Technologies for exceptions that have been approved under this policy.

E. Ongoing and Emerging Technology Threats

1. The Chief Information Security Officer in coordination with the UT Health IT Department shall implement the removal and prohibition of technology as published by DIR.

2. The Chief Information Security Officer in coordination with the UT Health IT Department may prohibit technology threats in addition to those identified by DIR.

F. Policy Compliance

All employees, contractors and users of Information Resources must agree to abide by the Acceptable Use Policy, including acknowledgement of restrictions on the use of Prohibited Technology.

G. Exceptions

Exceptions to the ban on prohibited technologies may only be approved by UT Health San Antonio's President or U.T. System Chancellor.

## V. Definitions

*When used in this document, the following words have the meaning set forth below unless the context requires a different meaning.*

Confidential Data – information that is required by federal law, state law, U.T. System policies, Regents' Rules, UT Health San Antonio policies or contract terms to be maintained in a confidential manner.

Information Resources – UT Health San Antonio owned or controlled technology hardware, software and data that are employed, designed, built, operated and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contracts. This includes the data, mechanisms, and processes for the transportation of data, and the media in which the data resides.

Mobile Device – a computing device with some or all of the following characteristics: small form factor, network interface for internet access, built-in data storage, applications available through multiple external methods (such as an "app store") and/or synchronization of data to an external location.
Personally Owned – includes assets which are not owned or managed by UT Health San Antonio.

Prohibited Technologies – software, applications, systems, platforms, hardware, and other digital resources that are prohibited by the State of Texas and/or UT Health San Antonio.

## VI. Related References

Institutional Handbook of Operating Policies
5.8.10 Information Resources Acceptable Use and Security Policy

## VII. Review and Approval History

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

| Effective Date | Action Taken | Approved By | Approved Date |
|---|---|---|---|
| 12/2/2024 | Policy Origination | Executive Committee | 12/2/2024 |
| | | | |
| | | | |