Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Prohibited Technology**
Regulation and Procedure Number:	**URP: 04.796**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

Texas Woman's University ("TWU" or "University") seeks to maintain policies and procedures in compliance with federal, state, and local laws and regulations. Governor Greg Abbott required all state agencies to ban the video-sharing application TikTok from all state-owned devices and networks over the Chinese Communist Party's ability to use the application for surveilling Texans. Governor Abbott also directed the Texas Department of Public Safety ("DPS") and the Texas Department of Information Resources ("DIR") to develop a plan providing state agencies guidance on managing personal devices used to conduct state business.

The State of Texas has published a list of prohibited technology and objectives to prevent the use of these technologies on state-owned, TWU-owned and personally-owned devices. This University Regulation and Procedure ("URP") outlines TWU's policy for implementing safeguards around prohibited technologies, protecting TWU-owned devices and infrastructure, and managing personal devices used to conduct TWU business.

The scope of these regulations and procedures is applicable to all Information Resources owned or operated by TWU and all technology-enabled personal devices owned by an individual User. All Users are responsible for adhering to these regulations and procedures. If needed or appropriate, information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures. The Policy Owner, as defined in URP 01.320: University Policy Development and Implementation, is responsible for managing the development, documentation, and dissemination of this URP.

APPLICABILITY

This policy is applicable to TWU Employees, University Affiliates, and Guests.

DEFINITIONS

1. “Employee” means any individual at TWU who is hired in a full-time, part-time, or temporary capacity in a faculty or staff position, or in a position where the individual is required to be a student as a condition of employment.

2. “Guests” means any individual not affiliated with TWU.

3. “Information Resources” means an element of infrastructure that enables the transaction of data, designed to provide content and information services to Users. Information Resources include information in electronic, digital, or audiovisual format and any hardware or software that store and use such information (i.e., electronic mail, local databases, externally accessed, CD-ROM, motion picture film, recorded magnetic media, photographs, digitized information, voice mail, faxes). This definition also includes computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, cloud services, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus. Additionally, Information Resources includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

4. "Prohibited Technologies" means all software and hardware products on the DIR prohibited technology list. "Prohibited Technologies" shall refer to TikTok and any additional hardware or software products added to the Prohibited Technologies list (*See* References).

5. “TWU Business” means accessing any TWU-owned data, applications, non-public facing communications, TWU email, Voice Over IP (“VoIP”), Short Message Service (“SMS,” e.g. texting or messaging), video conferencing, and any other TWU databases or applications.

6. “University Affiliate” means any individual associated with TWU in a capacity other than as a Student or Employee who has access to TWU resources through a contractual arrangement or other association. This includes the following individuals:

    a. Contractors and Vendors: an individual, business, or governmental entity that has a fully executed contract to provide

goods or services to TWU. This includes employees of contractors or vendors and independent contractors.

b. Employee of a Governmental Agency: an individual employed by a federal or Texas state agency.

c. Employee of a TWU-Affiliated Institution: an individual who works for organizations that are tightly aligned with the University.

d. Pre-Employment Individual: an individual who will be hired by the University and the hiring department has sponsored their access to TWU resources.

e. Other University Affiliate: any individual who does not fit into any other category and needs access to TWU resources.

7. "Users" means TWU employees, contractors, vendors, or other people using a TWU Information Resource.

REGULATION AND PROCEDURE

I. Objectives

To protect the State's sensitive information and critical infrastructure from technologies that pose a threat to the State of Texas, this URP outlines the following objectives which must be implemented by TWU:

A. Ban and prevent the download or use of prohibited technologies on any TWU-owned device. This includes all TWU-owned cell phones, laptops, tablets, desktop computers, and other devices capable of internet connectivity.

B. Prohibit Employees and University Affiliates from conducting TWU Business on prohibited technology-enabled personal devices.

C. Identify sensitive locations, meetings, or personnel within TWU that could be exposed to prohibited technology-enabled personal devices. Prohibited technology-enabled personal devices must be prohibited from entering or being used in these sensitive areas.

D. Implement network-based restrictions to prevent the use of prohibited technologies on TWU networks by any device.

E. Coordinate the incorporation of other technology providers as necessary, including any apps, services, hardware, or software that pose a threat to the State's sensitive information and critical infrastructure.

II. TWU-Owned Devices

A. Except where approved exceptions apply, the use or download of prohibited applications or websites is prohibited on all TWU-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

B. TWU IT Solutions shall identify, track, and control TWU-owned devices to prohibit the installation of or access to all prohibited applications. This includes the various prohibited applications for mobile, desktop, or other internet capable devices.

C. IT Solutions shall manage all TWU-owned mobile devices by implementing the security controls listed below:

1. Restrict access to "app stores" or non-authorized software repositories to prevent the install of unauthorized applications;

2. Maintain the ability to remotely wipe non-compliant or compromised mobile devices;

3. Maintain the ability to remotely uninstall un-authorized software from mobile devices; and

4. Deploy secure baseline configurations, for mobile devices, as determined by TWU.

III. Personal Devices Used for TWU Business

Employees and University Affiliates may not install or operate prohibited applications or technologies on any personal device that is used to conduct TWU Business. TWU Business includes accessing any TWU-owned data, applications, non-public facing communications, TWU email, Voice Over IP ("VoIP"), Short Message Service ("SMS," e.g. texting or messaging), video conferencing, and any other TWU databases or applications.

IV. Identification of Sensitive Locations

A. Sensitive locations must be identified, cataloged, and labeled by TWU. A sensitive location is any area with specific compliance requirements mandating limited access, such as a sensitive compartmentalized information facility ("SCIF").

B. Prohibited technology-enabled devices may not enter sensitive locations.

C. Guests granted access to secure locations are subject to the same limitations as University Affiliates and Employees on prohibited technology-enabled devices when entering secure locations.

V. Network Restrictions

A. DIR has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, TWU will also implement additional network-based restrictions to include:

1. Configure agency firewalls to block access to statewide prohibited services on all TWU technology infrastructures, including local networks, wide area network ("WAN"), and virtual private network ("VPN") connections; and

2. Prohibit personal devices with prohibited technologies installed from connecting to TWU technology infrastructure or state data.

VI. Ongoing Emerging Technology Threats

New technologies will be added to the list after consultation between DIR and DPS (*See* References). IT Solutions will implement the removal and prohibition of any listed technology and may prohibit technology threats in addition to those identified by DIR and DPS.

VII. Exceptions

A. Exceptions to the ban on prohibited technologies may only be approved by the Chancellor and President ("Chancellor"). This authority may not be delegated. All approved exceptions to the TikTok prohibition or other statewide prohibited technology must be reported to DIR.

B. Exceptions to the policy will only be considered when the use of prohibited technologies is required for a specific TWU Business need, such as enabling criminal or civil investigations or for sharing of information to the public during an emergency. For personal devices used for TWU Business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period of time. To the extent practicable, exception-based use should only be performed on devices that are not used for other TWU Business and on non-TWU networks. Cameras and microphones should be disabled on devices for exception-based use.

VIII. Compliance

Employees that violate this policy are subject to corrective and disciplinary action, including and up to dismissal, in accordance with TWU's URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes and URP 05.600: Staff Standards of Conduct and Disciplinary Process. TWU may also take corrective action against interns, volunteers, contract employees, contractors, and/or consultants that violate this policy, including and up to termination of TWU's relations or access with that individual or entity.

REVIEW

This policy will remain in effect and published until it is reviewed, updated, or archived. This policy is to be reviewed once every six years. Interim review may be required as a result of updates to federal and state law or regulations, Board of Regents policies, or internal processes or procedures.

REFERENCES

DIR Prohibited Technologies

URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes

URP 05.600: Staff Standards of Conduct and Disciplinary Process

FORMS AND TOOLS

None

Publication Date: 06/02/2023

Revised: (MM/DD/YYYY)