TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology **NUMBER: 04.06.32**
AREA: Computer and Information Technology
TITLE/SUBJECT: Prohibited Technologies Security Policy

I. POLICY STATEMENT:

On December 7, 2022, Governor Greg Abbott required all state agencies to ban the video-sharing application TikTok from all state-owned and state-issued devices and networks. Governor Abbott also directed the Texas Department of Information Resources ("DIR") to develop a model plan providing state agencies guidance on managing personal devices used to conduct state business.

II. PURPOSE:

This Policy outlines the responsibilities of all users of Texas Southern University ("University") owned or issued equipment, devices, and related University networks. The University is responsible for ensuring that all University networks and resources are secure and protected against damage, theft, unauthorized surveillance, or corruption by individuals or entities, internal or external to the University.

III. DEFINITIONS:

1. Equipment or Device: This includes all cell phones, laptops, tablets, desktop computers and other devices capable of internet connectivity.

2. Official Business: Includes accessing any state-owned data, applications, email accounts, non-public facing communications, state email, VoIP, SMS, video conferencing, CAPPS, Texas.gov, and any other state databases or applications.

3. Prohibited Technologies: Includes software, applications, and developers to the video-sharing application TikTok. Throughout this Policy, Prohibited Technologies shall refer to any additional hardware or software products added to this Policy.

4. University Equipment and Device: This includes all cellular phones, laptops, tablets, desktop computers and other devices capable of internet connectivity which were - (i) purchased by, and/or (ii) issued by - the University. The term "purchased by" includes the University providing a monetary allowance for such Equipment and Device. *See* MAPP 03.02.04 – Allowances for Communication Devices.

5. University Network: Wired or wireless network used for email, VoIP, data, voice, and video communications under the control of the University.

6. User: An individual (including staff, faculty, student, consultant, contractor, and volunteer) who accesses University Network or operates University Equipment or Device.

IV. SCOPE:

1. Application: This Policy applies to all Users of University Network as well as University Equipment and Device. All Users are responsible for complying with the terms and conditions of this Policy.

2. Exceptions: Exceptions to the Policy will only be considered when the use of prohibited technologies is required for a specific business need, such as enabling criminal or civil investigations or for sharing of information to the public during an emergency. Approval for this limited exception lies with the Chief Technology Officer in consultation with the V.P. of Business and Finance/CFO and Compliance Officer.

V. POLICY PROVISIONS:

1. Aside from an approved exception under Section IV, ¶2 above, the use or download of Prohibited Technologies or websites is prohibited on all University Equipment and Device.

2. To provide protection against ongoing and emerging technological threats to the University's sensitive information and critical infrastructure, the University will regularly monitor guidance from the Department of Public Safety and DIR (https://dir.texas.gov/information-security/prohibited-technologies) to evaluate any additional technologies posing concerns for inclusion in this Policy.

3. The University may add other software and hardware products with security concerns to this Policy and may remove prohibited technologies which are on the DIR prohibited technology list. Any such inclusion regarding technology threats will be listed on the Office of Information Technology's ("OIT") website.

VI. PROCEDURES:

1. OIT shall identify and track inventory of University Equipment and Device to ensure against the installation of or access to Prohibited Technologies.

2. All Users of University Equipment and Device shall sign a document confirming their understanding of, and adherence to this Policy.

3. OIT will manage all University cellular phones by implementing the security controls listed below:

   a. Restrict access to "app stores" or non-authorized software repositories to prevent the install of unauthorized applications.
   b. Maintain the ability to remotely wipe non-compliant or compromised cellular phones.
   c. Maintain the ability to remotely uninstall un-authorized software from cellular phones.
   d. Deploy secure baseline configurations, for cellular phones, as determined by the University.

4. OIT will implement network-based restrictions to include:

    a. Configuration of University firewalls to block access to University and statewide prohibited services on all University technology infrastructures, including local networks, WAN, and VPN connections.
    b. Providing access to Prohibited Technologies with the requisite approval after consultation.

VII. POLICY COMPLIANCE:

1. All Users must adhere to all provisions of this Policy, as well as applicable security standards included in the Security Standards Policy. *See* MAPP 04.06.22.

2. All Users shall acknowledge their understanding of, and adherence to this Policy. Compliance with this Policy will be verified through various methods, including but not limited to, annual training and random compliance checks.

3. All Users expressly consents to monitoring on the part of the University for these purposes and is advised that if such monitoring reveals possible evidence of criminal activity or misuse of state resources, the evidence will be referred to appropriate officials, including law enforcement officials.

4. Users who violate the provisions of this Policy shall be subject to cancellation or suspension of related account(s), cancellation or suspension of monetary allowance, suspension with or without pay, involuntary employment dismissal, or other disciplinary action by the University. *See* MAPP 02.05.03 – Discipline and Termination Policy; MAPP 03.02.04 – Allowances for Communication Devices.

REVIEW AND RESPONSIBILITIES:

Responsible Party: Chief Technology Officer

Review: Every 3 years, on or before September 1st

APPROVALS:

Arman Rashid, Chief Technology Officer

Hao Le, Chief Compliance Officer

Lesia L Crumpton-Young

Dr. Lesia Crumpton-Young, President

02/13/2023

Effective Date