I. POLICY STATEMENT:

On December 7, 2022, Governor Greg Abbott issued a directive requiring all state agencies to prohibit certain applications, including TikTok, on 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. The 88th Texas Legislature subsequently codified and expanded these requirements through Senate Bill 1893, now reflected in Texas Government Code Chapter 620, which governs the use of covered applications and prohibited technologies by state agencies and institutions of higher education. In accordance with these requirements, Texas Southern University (the "University") prohibits the procurement, installation, and use of covered applications and prohibited technologies, as identified by the Texas Department of Information Resources, to protect the University's information resources, sensitive data, and critical infrastructure.

II. PURPOSE AND SCOPE:

This Policy outlines the responsibilities of all users to ensure that all University networks and information resources are secure and protected against unauthorized access, data theft, unauthorized surveillance, damage or corruption by individuals or entities, internal or external to the University.

This policy applies to all University full and part-time employees, students, contractors, consultants, interns (paid or unpaid), volunteers, guests, visitors, and all other us**ers** of the University Network or University Equipment and Devices.

III. DEFINITIONS:

1. Covered Application: As defined in Texas Government Code, Section 620.001(1), the social media service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited, or a social media application or service specified by proclamation of the governor under Texas Government Code, Section 620.005.
2. Equipment or Device: This includes all cell phones, laptops, tablets, desktop computers and other devices capable of internet connectivity.

3. Official Business: Includes accessing any state-owned data, applications, email accounts, nonpublic facing communications, state email, VoIP, SMS, video conferencing, CAPPS, Texas.gov, including **LMS (Canvas),** and any other state databases or applications.

4. Prohibited Technologies: Includes any software, applications, and developers, **hardware, or manufacturers, other than those defined as a Covered Application, identified on the DIR Covered Applications and Prohibited Technologies List, as amended**. Throughout this Policy, Prohibited Technologies shall refer to any additional hardware or software products added to this list. The University adopts the DIR Covered Applications and Prohibited Technologies List, as amended.

5. 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.

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

7. User: An individual (including **full and part-time employees**, faculty, student, consultant, contractor, **paid or unpaid intern,** volunteer, guest, and visitor) who accesses University Network or operates a University Equipment or Device.

IV. POLICY PROVISIONS:

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

2. In order to provide protection against ongoing and emerging technological threats to sensitive information and critical infrastructure, the University adopts **the DIR Covered Applications and Prohibited Technologies List, as amended.** The University will regularly monitor guidance from the Department of Public Safety and DIR (https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies) to evaluate any additional technologies posing concerns for inclusion in this Policy.

3. Personal devices with any Prohibited Technology or Covered Application installed are prohibited from connecting to any University Network. The University shall implement network-based restrictions to block traffic to prohibited services for all devices on the University technology infrastructure.

4. **Purchasing Restrictions:** The University will not purchase or reimburse the purchase of any Covered Applications or Prohibited Technologies.

5. The University may add other software and hardware products with security concerns to this Policy and may remove and prevent installation and use of Prohibited Technologies and Covered Applications as they are added are on the DIR Prohibited Technology list. (https://dir.texas.gov/information-security/prohibited-technologies or specified by proclamation of the governor. Any such inclusion regarding technology threats will be listed on the Office of Information Technology's ("OIT") website.

V. 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 **Covered Applications and Prohibited Technologies on** all University technology infrastructures, including local networks, WAN, and VPN connections.
   b. Providing **separate network for access to Covered Applications and Prohibited Technologies when approved by the University President.**

VI. 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 consent to monitoring on the part of the University for these purposes and are 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. Personal devices used to conduct official University business may not access or install Covered Applications or Prohibited Technologies while connected to the University network or when accessing state data or systems.

5. 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.

6. Operational enforcement of this policy is within the Human Resources Department stewardship with assistance from the Compliance office. *See* MAPP 02.05.03 – Discipline and Termination Policy; MAPP 03.02.04 – Allowances for Communication Devices.

VII. EXCEPTIONS

1. **Covered Application Exceptions:** The University may permit exceptions for Covered Applications **only** for (a) providing law enforcement, or (b) developing or implementing information security measures. Documentation of risk mitigation is required.

2. **Prohibited Technologies Exceptions:** Exceptions for Prohibited Technologies may be permitted for law enforcement, public safety, legal adjudications, intellectual property enforcement, or approved research and teaching (provided use is on an isolated, University-issued device).

3. **Approval Authority:** All exceptions must be approved by the **University President**. This authority may not be delegated.

4. **Reporting:** All exception requests must be submitted to the **Office of Information Technology (OIT)** for review and final submission to the President. All approved exceptions must be reported to the **Texas Department of Information Resources (DIR)**.