# STATE OF ALABAMA

## INFORMATION TECHNOLOGY POLICY

| Policy 601: Restricted Applications - TikTok | | |
|---|---|---|
| Document/Version: 601-01 | Effective Date: 12/12/2022 | Reviewed: DEC 2022 |
| Version Date: 12/12/2022 | Compliance Date: 12/12/2022 | Next Review: DEC 2025 |

OBJECTIVE

Address restrictions related to the use of social media application TikTok.

AUDIENCE

Intended for all Personnel at all levels of the executive branch.

DEFINITIONS

TikTok: a social media platform for sharing short user-submitted videos. The video hosting service is owned by ByteDance, a Chinese company.

STATEMENT OF POLICY

When personnel access social media and networking sites, the information shared is not private. This includes information about the device used to connect, the IP address, user location, and other info that is shared without user interaction or knowledge. What the site or application owner does with the data they collect is usually stated in their privacy policy and posted where the end-user can read and decide whether to accept the risk.

In a letter to nine U.S. Senators dated June 30, 2022, TikTok admitted that China-based employees can access U.S. user data, including data stored in the continental U.S. This data access represents a significant risk to end-user privacy, and by using state IT resources to access TikTok, the end-user is also placing the state at risk.

It is therefore the policy of OIT that:

a) The social media application known as "TikTok" shall be restricted from download, installation, or use on any state-owned devices and/or networks.

b) For personal safety and privacy, it is recommended that TikTok be uninstalled/deleted from personally owned devices even if those devices are not used on the state's networks (including Wi-Fi).

OIT RESPONSIBILITIES

OIT shall:

O.1 At the state network perimeter, update firewall rules to block both egress and ingress traffic from all domains, TCP/IP addresses/blocks and known hostnames uniquely used by TikTok.

O.2 Ensure that wireless access points similarly restrict traffic from accessing TikTok.

AGENCY RESPONSIBILITIES

Agencies responsible for their own network shall:

A.1 Implement firewall rules to block both egress and ingress traffic from all domains, TCP/IP addresses/blocks and known hostnames uniquely used by TikTok. This information is available via Netify: (https://www.netify.ai/resources/applications/tiktok).

For next-generation firewall (NGFW) devices, existing policy sets may be available from the NGFW vendor to implement these as a single policy set. Consult your firewall vendor(s) to determine whether such a pre-defined policy set is available.

A.2 Implement mobile device management (MDM) software on all State-owned mobile devices and implement policy prohibiting the TikTok application from being installed or executed on the device. Where possible, block TikTok application download from app stores including Apple and Google app stores and device-specific sources such as Samsung Galaxy Store.

A.3 Ensure end-users are made aware of the risks pertaining to the use of TikTok, the risk of social media use in general, and the restrictions implemented to offset those risks.

A.4 Perform frequent health checks to ensure that blocking rules are functioning as desired.

A.5 Monitor attempts to access restricted social media sites. This information may be used to determine the need for additional security awareness training.

COMPLIANCE CHECKS

The following checks shall be used to ensure effective policy implementation:

C.1 Examine security and privacy policies pertaining to restrictions on use of social media applications and websites.

C.2 Agencies shall provide to OIT (upon request) attestation indicating acknowledgement of, implementation of, and evidence of compliance with this policy. Evidence may include firewall logs indicating blocked access attempts.

## SUPPORTING DOCUMENTS

The following documents support this policy:

- Policy 660: System Use
- Policy 638: Mobile Device Access Control

## AUTHORITY AND APPLICABILITY

The authority of the Office of Information Technology (OIT) to create and enforce policies relating to the management and operation of IT by State agencies, and exceptions to such authority, are derived from:

*Articles 8 and 11 of Chapter 4 of Title 41, and Chapter 28 of Title 41, Code of Alabama 1975 (See Acts 2013-68 and 2017-282).*

The requirements and responsibilities defined in enterprise policies generally apply to all Executive Branch departments, agencies, offices, boards, commissions, bureaus, and authorities (referred to generally as ***agency*** or ***agencies***) and authorized individuals in the employment of the State of Alabama responsible for the management, operation, or use of IT resources including contractors and retired state employees. This scope of authority is generally referred to as ***enterprise*** throughout IT policy documentation to distinguish it from broader statewide policy set by the Governor, Legislature, or other entities, and from narrower agency-level policy which applies only to individual agencies.

## DOCUMENT CHANGE HISTORY

| Version | Version Date | Comments |
|---|---|---|
| 601-01 | 12/12/2022 | Initial version |
| | | |
| | | |