# TECHNICAL BULLETIN

# Executive Order 2023-10

RE:  Removal of TikTok from State-owned and State-leased IT and personal devices used for State work

This document provides detailed steps taken and recommended actions for state agencies on their implementation and enforcement of this Executive Order on agency managed Services/Devices.

**Background**

On April 4, 2023, Governor Katie Hobbs signed Executive Order 2023-10 titled “Protecting the State’s Cybersecurity Interests”.  This orders the removal of TikTok from State-owned and State-leased IT and personal devices used for State work, as well as reporting annually on “...identifying other applications that pose potential cybersecurity threats and that may need to be similarly restricted…”

The full order can be found on the Governor’s office website as of this writing: https://azgovernor.gov/office-arizona-governor/executive-order/executive-order-2023-10

**Initial Action**

ADOA-ASET partnered with the Arizona Department of Homeland Security (AZDOHS), completed the task, and developed the following solution to implement, enforce, and work with state agencies to effectively follow this Executive Order.

The solution includes changes to AZNet Managed Firewalls, AZDOHS Zscaler (Web Content Filter), Google Tag Manager, and Tanium. The change in the State Firewall is Enterprise-wide; however, agency managed firewalls require agency action.

## Actionable Items

### Computing and other devices on State Network

#### Tanium

Systems and procedures to use on Tanium, the State's current platform to secure endpoint devices such as desktops, laptops, etc. The following steps are used to meet the directive requirements:

1. Login to Tanium,
2. Go to the Interact Modules and look for "Saved Questions"
3. In the Saved Questions section, click on the search box and type in "TikTok"
4. You will see the saved question "AD-TikTok Appx is installed"
5. The question will provide the necessary information on the computers and user names.
6. If you wish to remove TikTok, you can deploy a package to target those endpoints.
7. The software package is available in the Deploy Module > Software > AD Remove TikTok APPX v1.0

#### Mobile Devices

The removal of TikTok from, and the monitoring for TikTok use, on mobile devices used by and on state networks. This requires implementation on IOS, the Apple platform, and Android.

These instructions are the general steps to restrict TikTok from state-owned mobile devices.

GOOGLE ENTERPRISE MOBILITY MANAGEMENT (EMM) SOLUTION (Android & IOS)

In order to restrict the installation of applications on a mobile device using the State's current Google Enterprise Mobility Management (EMM), the devices have to be in a fully managed (for Apple, "supervised"), company-owned state.

1) End user devices need to be configured for Advanced Management.
2) Android devices need to be configured to only install "Allowed Apps".
3) iOS devices need to be configured to allow the installation of apps, but restricted from installing apps from the App Store. This configuration will only permit iOS devices to install apps in Google Workspace that are approved by the state and can be installed via the Google Device Policy App.

Below are the instructions for getting devices setup as fully managed (supervised) company-owned devices.

## APPLE DEVICES

In order to effectively manage Apple iOS devices, agencies need to collaborate with their wireless carriers to connect to ADOA's Apple Business Manager (ABM). ABM is a user-friendly web portal that seamlessly integrates with the State's Google EMM, enabling easy and comprehensive management of iOS devices. Through ABM, agencies can ensure that all their current and future devices are incorporated into ADOA's ABM. Additionally, ABM offers the capability to generate managed Apple IDs associated with ADOA's ABM.

Since Google's EMM only allows for one ABM, other agencies seeking full device management will need to have their device fleet integrated into ADOA's ABM. Alternatively, agencies would need to seek out their own EMM/MDM solution in order to integrate their instance of ABM. Another alternative is for the state to adopt an alternate solution that permits the integration of multiple ABMs.

The primary authority at the agency's wireless carrier must complete the necessary paperwork to authorize the contracted fleet of devices for management via ABM.

The agency has the option to contact the carrier, requesting that specific iOS devices be managed through ABM. Typically, a CSV file containing device-specific data is provided to the carrier to indicate which devices should be imported. It is also possible to request that future devices or all devices be incorporated into ABM.

ADOA's ABM instance is already linked to the State's Google EMM. Once devices are imported into ADOA’s ABM, they will automatically be imported as company-owned devices in Google EMM.

If the device is brand new, a user only needs to log in with an Apple ID, preferably one created using their state email address.  If the device is currently in use, the device would need to be factory reset in order for device policy to take effect.

The Google Device Policy App should be automatically installed, at which point the end user can log into the app using their Google Workspace account.

This configuration ensures that iOS devices are fully managed and allows the Google MDM to impose necessary restrictions on the app store.

## ANDROID DEVICES

There are multiple approaches for setting up Android devices as company-owned devices.

1. User-Initiated Enrollment with Company-Owned Designation:
    a. Users receive their mobile devices and use their Google Workspace account for the initial device enrollment.
    b. During the enrollment process, users are prompted to choose between a user-owned or company-owned device, and must select “company-owned”.
    c. When they select “company-owned”, the device will be managed and Google Workspace account settings will reflect this designation.
2. Adding Serial Numbers to Google EMM Prior to User Enrollment:
    a. Administrators need to add the serial numbers of mobile devices to the Google EMM via a CSV file to designate them as company-owned before users enroll with their Google Workspace accounts.
    b. Once the device is registered, Google will automatically configure it as a company-owned device.
    c. If a user is already enrolled, they will need to factory reset the device for the new company-owned settings to take effect.
3. Android Zero Touch Enrollment (Similar to ABM for Android):
    a. Similar to Apple Business Manager (ABM), this method requires coordination with the wireless carrier or reseller to synchronize devices into the Android Zero Touch Portal.
    b. The devices will be pre-configured with the necessary settings and policies for company-owned use.

For agencies that prefer to use their own Mobile Device Management (MDM) and ABM:

- These agencies need to complete a risk acceptance request form, as it involves changing security controls in their Organizational Unit (OU) within Google Workspace.
- This change ensures that Google Workspace does not push a device policy to the agency's mobile devices, allowing them to apply a device policy using their own MDM solution.

## ZScaler:  State Network and Internet Use

In addition to the changes applied by ADOA and AZDOHS to add TikTok to the Blocked Application list on State Firewalls as well as AZDOHS managed Zscaler, Agencies are encouraged to apply relevant changes for monitoring and blocking TikTok usage to their agency managed Firewall and ZScaler systems.

To implement changes to ZScaler platform, please use the instructions.

## Websites

### Google Tag Manager

Instructions on the use of Google Tag Manager (GTM) to remove and stop the addition of marketing, advertising, and tracking tags related to TikTok.  These instructions should be provided to all State agencies and departments.  Agencies and departments should also provide these instructions to any third parties who handle their marketing, advertising, and tracking on websites and web based platforms.

1. Instruct all users who have access to make changes within Google Tag Manager about the prohibition.
2. Remove any active TikTok tags from GTM https://support.google.com/tagmanager/answer/12329709?hl=en&sjid=17873295500965076958-NA
3. Ensure all active tags are periodically reviewed to ensure compliance with the executive order. https://support.google.com/tagmanager/answer/12347177?hl=en&ref_topic=12403939&sjid=17873295500965076958-NA
4. Ensure the GTM Account Administrator is a State Employee https://support.google.com/tagmanager/answer/6107011?hl=en&sjid=17873295500965076958-NA
5. Ensure the GTM Account Administrator has Container Notifications turned on. https://support.google.com/tagmanager/answer/9713667?hl=en&sjid=17873295500965076958-NA
6. If using the Google Marketing Platform (paid version) and Google Tag Manager 360, ensure the GTM Account utilizes the Approval Queue and a State Employee is designated for approving all tags and changes. https://support.google.com/tagmanager/answer/6107163?hl=en&sjid=17873295500965076958-NA
7. Instruct all marketing and advertising vendors that advertising and analytics gathering using TikTok technologies is prohibited.
8. Ensure any activity by a third party vendor with access to GTM is monitored for compliance. https://support.google.com/tagmanager/answer/12347177?hl=en&ref_topic=12403939&sjid=17873295500965076958-NA

**References:**

Executive Order 2023 “Protecting the State’s Cybersecurity Interests”, April 4, 2023, https://azgovernor.gov/office-arizona-governor/executive-order/executive-order-2023-10

The following documents and procedures were created and defined to remove TikTok as directed by the Executive Order and further manage the monitoring and continual removal of TikTok from any new devices:

- Addressing TikTok On Mobile Devices https://aset.az.gov/sites/default/files/2023-06/Addressing%20TikTok%20for%20Mobile%20Devices.pdf
- EO_2023-10 compliance: Recommended method for blocking TikTok in Zscaler Internet Access https://aset.az.gov/sites/default/files/2023-06/EO_2023-10%20compliance_%20Recommended%20method%20for%20blocking%20TikTok%20in%20Zscaler%20Internet%20Access.pdf
- Google Tag Manager(GTM) and TikTok https://aset.az.gov/sites/default/files/2023-06/GTM%20and%20TikTok.pdf
- AZDOHS policies page containing the risk acceptance form https://azdohs.gov/information-security-policies-standards-and-procedures