Australian Government
Attorney-General's Department

Protective Security Policy Framework
Direction 001-2023

Direction on the TikTok application

Published: 4 April 2023

The Protective Security Policy Framework (PSPF) applies to non-corporate Commonwealth entities subject to the *Public Governance, Performance and Accountability Act 2013*.

The PSPF provides that, having considered advice from lead protective security entities, the Secretary of the Attorney-General's Department may issue a direction to accountable authorities to manage a protective security risk to the Commonwealth.[1] The accountable authority of each entity must adhere to any direction issued.[2]

PSPF Direction 001-2023 deals with the risks of the TikTok application. The TikTok application poses significant security and privacy risks to non-corporate Commonwealth entities arising from extensive collection of user data and exposure to extrajudicial directions from a foreign government that conflict with Australian law.

On advice from lead protective security entities, I have determined that the installation of the TikTok application on government devices poses a significant protective security risk to the Commonwealth.[3]

Entities **must prevent** installation and remove existing instances of the TikTok application on government devices, unless a **legitimate business reason** exists which necessitates the installation or ongoing presence of the application.

The Chief Security Officer of the entity **must** approve any legitimate business reason for the use of the TikTok application on government devices and ensure the following **mitigations are in place** to manage security risks:

- Ensure the TikTok application is installed and accessed only on a separate, standalone device without access to services that process or access official and classified information.
- Ensure the separate, standalone device is appropriately stored and secured when not in use. This includes the isolation of these devices from sensitive conversations and information.
- Ensure metadata has been removed from photos, videos and documents when uploading any content to TikTok.
- Minimise, where possible, the sharing of personal identifying content on the TikTok application.
- Use an official generic email address (for example, a group mailbox) for each TikTok account.
- Use multi-factor authentication and unique passphrases for each TikTok account.
- Ensure that devices that access the TikTok application are using the latest available operating system in order to control individual mobile application permissions. Regularly check for and update the application to ensure the latest version is used.
- Only install the TikTok application from trusted stores such as Microsoft Store, Google Play Store and the Apple App Store.

[1] PSPF policy: Role of accountable authority at paragraph 3.
[2] PSPF policy: Role of accountable authority at B1.
[3] This direction applies only to the TikTok application and does not restrict access to TikTok through the use of a web interface (for example, accessing through a website).

- Ensure only authorised users have access to corporate TikTok accounts and that access (either direct or delegated) is revoked immediately when there is no longer a requirement for that access.
- Carefully and regularly review the terms and conditions, as well as application permissions with each update, to ensure appropriate risk management controls can be put in place or adjusted as required.
- Delete the TikTok application from devices when access is no longer needed.

Further information about these mitigations are available in ASD's Information Security Manual.

This direction does not impact the use of the TikTok application on personal devices. However, entities that **accept the risks** of the use of personal devices to access official or classified system data (i.e. pursuant to remote access arrangements including Bring Your Own Device (BYOD) or equivalent policies), **must** provide access to that data through non-persistent and full remote access solutions, approved by the Chief Security Officer, as opposed to using the native storage and applications on the personal device.

Entities should take the necessary steps to ensure they adhere to this direction **as soon as practicable**.

Legitimate business reason means a need to install or access the TikTok application on a government device to conduct business and/or achieve a work objective of an entity. A legitimate business reason would include:

- where the application is necessary for the carrying out of regulatory functions including compliance and enforcement functions
- where an entity requires research to be conducted or communications to be sent to assist with a work objective (for example, countering mis- or dis-information), or
- where an entity must use the application to reach key audiences to undertake marketing or public relations activity on behalf of the entity.

As technologies continue to develop, new risks relating to technology may emerge and require further consideration. Entities are encourages to familiarise themselves with ASD's *Cyber Supply Chain Risk Management* and *Identifying Cyber Supply Chain Risks*, as well as continue to adopt the Information Security Manual.

For more information or support please contact PSPF@ag.gov.au or 02 6141 3600.

Katherine Jones
Secretary Attorney-General's Department