Direction 1-2023

Direction on the use of TikTok

Department of Premier and Cabinet

Tasmanian Government

Direction on the use of TikTok

Tasmania's Protective Security Policy Framework (TAS-PSPF) currently applies to Tasmanian Government agencies and their subsidiaries, per section 1.3 of the framework.

Under the **TAS-PSPF policy: Establish security governance (GOVSEC-1)**, Accountable Authorities must action their roles and responsibilities, which includes adhering to any direction issued under the TAS-PSPF.

This direction (Direction 1-2023) addresses the use of TikTok on Tasmanian Government issued devices. Based on the accepted security risks associated with TikTok, being that the application poses significant security and privacy risks, I have determined that the installation of the application on Tasmanian Government issued devices is a risk to our state and national interests[1].

Required action: Prohibit the use of TikTok

The Accountable Authority must prevent the installation, and ensure removal of existing instances, of the TikTok application on Tasmanian Government issued devices[2]. This includes devices issued to all people within your agency[3].

Where the Accountable Authority identifies the use of TikTok necessary to conduct business and/or achieve a work objective of the agency, this use may be considered under a legitimate business exemption.

A legitimate business reason includes:

- where the application is necessary for the carrying out of regulatory functions including compliance and enforcement functions
- where an agency requires research to be conducted or communications to be sent to assist with a work objective (for example, countering mis- or dis-information), or

[1] This direction applies only to the TikTok application and does not restrict access to TikTok using a web interface (for example, accessing through a website).

[2] Except in circumstances where a legitimate business reason exists, necessitating the installation or ongoing presence of the application.

[3] Per the TAS-PSPF, 'people' is defined as:

> *Employees and contractors, including secondees and any service providers that an agency engages. It also includes anyone who is given access to Tasmanian Government assets.*

- where an agency must use the application to reach key audiences to undertake marketing or public relations activity on behalf of the agency.

The Accountable Authority must conduct a risk assessment, where a legitimate business reason to use TikTok has been identified. The Accountable Authority must approve any exemption to this ban and only in circumstances where the known and considered risks are outweighed by the benefit of continued use.

The Accountable Authority must ensure the known security risks are managed by implementing the following mitigations when authorising the use of TikTok:

- The TikTok application is installed and accessed on a separate, standalone device without access to services that process, or access, official and security classified information (i.e., no official email or other work-related applications).
- Any of these standalone devices are appropriately stored and secured when not in use, which includes the isolation of these devices from sensitive conversations.
- Remove metadata from photos, videos and documents when uploading any content to TikTok.
- Minimal sharing of personal identifying content on the TikTok application, where possible.
- Use an official generic email address (for example, a group mailbox) for TikTok accounts.
- Use multi-factor authentication and unique passphrases for TikTok accounts.
- The devices that access the TikTok application are using the latest available operating system to control individual mobile application permissions. Regularly check 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.
- Only authorised users have access to corporate TikTok accounts and their access (either direct or delegated) is revoked immediately when there is no longer a requirement for it.
- Regularly and carefully 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.

This direction is to be actioned as soon as practicable.

Further information regarding the mitigations outlined in this direction (Direction 1-2023) can be found in the Australian Cyber Security Centre's Information Security Manual .

For more information or support please contact Resilience and Recovery Tasmania via sem@dpac.tas.gov.au or (03) 6232 7979.

Note: Personal devices

This direction (Direction 1-2023) does not impact the use of the TikTok application on personal devices.

If you accept the risk of the use of employees' personal devices which access official or classified system data (for example pursuant to remote access arrangements, including Bring Your Own Device (BYOD)), you must protect that data according to the requirements of the Accountable Authority.

Authorisation

I, Jeremy Rockliff, the Premier of Tasmania and the authority of the TAS-PSPF, require Accountable Authorities to adhere to this direction issued on 4 day of June 2023.

Issued and authorised by:

Jeremy Rockliff MP
Premier

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7770

Email:
taspspf@dpac.tas.gov.au