SACSF/R3.0 - GOVERNMENT RULING ON CYBER SECURITY

SACSF Ruling 3 – TikTok use on South Australian Government devices

Purpose

This Ruling provides a direction to South Australian Government agencies under *SACSF Policy Statement 2.12 Mobile Device Management* on the use of the TikTok application on South Australian Government devices.

An assessment has been made that the TikTok application poses significant security and privacy risks and agencies must remove existing instances of TikTok and prevent the installation of TikTok on government issued devices.

Scope

The SA Cyber Security Framework applies to all South Australian Government public sector agencies (agencies), including administrative units, bodies corporate, statutory authorities, and instruments of the Crown as per the *Public Sector Act 2009*.

An SACSF Ruling is a mandatory application of a SACSF Policy Statement. This Ruling 3 relates to the following SACSF Policy Statement:

> **2.12: Mobile Device Management:** Technical and procedural controls must be in place to address the risks associated with the use of mobile devices including mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet connected devices.

This Ruling does not impact the use of the TikTok application on personal devices. However, agencies that accept the risks of the use of personal devices to access official, sensitive or security classified data (i.e. pursuant to remote access arrangements including Bring Your Own Device (BYOD) or equivalent), must formally assess the risk of TikTok as part of this policy position.

Ruling

Government agencies **must** prevent the installation and remove existing instances of the TikTok application on government devices (e.g. phones, tablets or computers), unless a **legitimate business reason** exists which necessitates the installation or ongoing presence of the application.

The Agency Security Executive and agency IT Security Advisor **must** be consulted in the assessment and approval of a **legitimate business reason**.

The following risk mitigations **must** be assessed and implemented within the context of the agency's ICT environment as part of the approval of a **legitimate business reason**:

- Ensure the TikTok application is installed and accessed only on a separate, standalone device without access to services that process, store or access official, sensitive or security classified government 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.
- 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.

Roles and responsibilities

Position title or unit/team	Listed responsibilities
Agency Chief Executive	Responsible for the effective implementation of, and compliance, with this Ruling within their agency.
Agency Senior Executives, Directors and Managers	Responsible for ensuring: • the Ruling is implemented and observed by staff • staff are fully informed of their obligations and responsibilities under the Ruling • any reporting requirements are met.
Agency Security Executives	Responsible for ensuring that the Ruling is implemented within the agency and that business processes support the Ruling requirements. Required to be consulted on and make informed, risk-based decisions on any requests for legitimate business use of TikTok on government devices.
Agency IT Security Advisor	Responsible for providing advice on application of this Ruling within the agency environment, and for providing advice on the risks to agency information and services. Required to be consulted on and provide informed, risk-based advice on any requests for legitimate business use of TikTok on government devices.
All agency staff	Required to comply with the Ruling and any related procedures, and to play an active role in ensuring the compliance of others.

Definitions

Term	Definition
Legitimate Business Reason	For the purposes of this Ruling, 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.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this standard. There is no specific impact on Aboriginal people.

Related documents

- South Australian Protective Security Framework
- South Australian Cyber Security Framework
- Australian Government Protective Security Policy Framework - Direction 001-2023
- Australian Cyber Security Centre - Security Tips for Social Media and Messaging Apps

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Cyber Security	Email: cybersecurityOCIO@sa.gov.au
Division: Office of the Chief Information Officer	Compliance: Mandatory
Review number: v1.0 FINAL	Date of approval: 5/4/2023
Next review date: 5/4/2024	