

Administrative Guidelines on improving the cyber security of Victorian Government systems and data

Number: 2023/01

Issue: 1.0

ADMINISTRATIVE GUIDELINES

(issued under section 36A of the *Public Administration Act 2004*)

Date: 03/07/2023

Number: 2023/01

IMPROVING THE CYBER SECURITY OF VICTORIAN GOVERNMENT SYSTEMS AND DATA

1. Introduction

- 1.1. Protecting Victorian Government systems and data is essential in creating a cyber safe Victoria and continuing to deliver safe and reliable government services.
- 1.2. Following reviews into the security risks of high-risk mobile applications and bring-your-own-device (BYOD) practices, the Victorian Government approved two policy guidelines to mitigate identified cyber security and data privacy risks:
 - *Guidelines on the use of the TikTok application*
 - *Guidelines on the use of the use of personal mobile devices to access official systems and data.*

2. Purpose of these Administrative Guidelines

- 2.1. These Guidelines set out the expectations for public service bodies and public entities to:
 - prevent installation and remove existing instances of the TikTok application (TikTok) on government-issued devices unless a legitimate business use reason is approved
 - conduct a thorough cyber security risk assessment to inform the establishment of a local BYOD policy. This expectation applies to any public service body or public entity that supports BYOD practices
 - identify, implement and monitor the effectiveness of the TikTok restrictions and the BYOD policy with its associated controls.

3. Application and commencement

- 3.1. These Guidelines apply to all public service bodies and public entities, as defined by the *Public Administration Act 2004*. Departments are asked to support communication of the guidelines to relevant portfolio entities.
- 3.2. Public service bodies and public entities are expected to manage the requirements of the Guidelines with their employees, contractors, consultants, vendors and any other parties who have access to Victorian Government owned network, data or devices.
- 3.3. Certain bodies are not bound by these Guidelines, including Special Bodies and Exempt Bodies as defined under the *Public Administration Act 2004*. Such bodies are still encouraged to review the risks and issues that inform the government's approach as set out in these Guidelines and consider whether it would be appropriate to act consistently with these Guidelines.
- 3.4. These Guidelines commence on the date they are issued.
- 3.5. Public service bodies and public entities should take the necessary steps to ensure they adhere to these guidelines as soon as practicable.

4. Guidelines on the use of TikTok

- 4.1. Public service bodies and public entities must prevent installation and remove existing instances of TikTok on government devices unless a legitimate business reason exists.
- 4.2. Public service bodies and public entities should update internal information technology and/or security policies and are encouraged to implement technical controls to prevent the use of TikTok on government devices.
- 4.3. Where TikTok needs to be removed by employees, contractors or consultants on Victorian government issued or owned devices, public service bodies and public entities should give reasonable and lawful directions for the person to do so.

Legitimate business use reasons for the TikTok application

- 4.4. Legitimate business use means a need to install or access the TikTok application on a government device to conduct business and/or achieve a work objective of a body or entity. TikTok should only be accessed or installed after an adequate risk assessment has been completed, mitigation strategies are implemented, and necessary internal agency approvals are provided.
- 4.5. Legitimate business use reasons may include:
 - where the application is necessary for the carrying out of law enforcement and 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, releasing government communications, countering mis- or dis-information), or
 - where an entity must use the application to reach key audiences to undertake education, child safety, staff safety, marketing or public relations activity on behalf of the entity.
- 4.6. Public service bodies and public entities may identify a legitimate business use that requires the installation or ongoing presence of TikTok. The relevant agency head of the public service body or public entity should ensure legitimate business use reasons are approved by the Chief Security Officer (or equivalent) of the body or entity and ensure the approved risk mitigations are in place:
 - ensure TikTok is installed and accessed only on a separate government issued, 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 TikTok
 - use an official generic email address (for example, a group mailbox) or Chief Security Officer (or equivalent) approved email account 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 to control individual mobile application permissions
 - regularly check for and update the application to ensure the latest version is used
 - only install TikTok 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
 - an appropriately qualified person regularly reviews the terms and conditions of use or installation of TikTok, as well as application permissions with each update,

to ensure appropriate risk management controls can be put in place or adjusted as required

- delete TikTok from devices when access is no longer needed.

5. Guidelines on the use of the use of personal mobile devices to access official systems and data

5.1. Public service bodies and public entities that support employees to use a personal device to access official systems and data, including (but not limited to) work-related emails, messages, documents or corporate applications, should:

- Ensure that use of a personal device to access official systems and data is governed by an approved bring-your-own-device (BYOD) policy, or similar acceptable use of Information Technology (IT) or information security policy, that outlines organisational expectations regarding:
 - device access controls – minimum expectations for device access (e.g., password and lock screen protections)
 - device physical security – procedures for reducing the risk of, and responding to, lost or stolen devices
 - employee engagement and changes of status – protocol for on-boarding and off-boarding employees involved in BYOD practices
 - ongoing employee education and training on cyber security – including advice on the safe use of social media and messaging applications and acknowledgement of BYOD security policy
 - compliance monitoring and reporting – arrangements for monitoring compliance with the policy
 - any other matters relevant to ensuring the confidentiality, integrity and availability of official systems and data.
- Ensure the policy reflects a thorough cyber security risk assessment that considers:
 - how threats, vulnerabilities and risks are identified and recorded
 - how threats, vulnerabilities and risks impact the protection of organisational employees, information and assets, and how they are being mitigated
 - the organisation's tolerance to security risks, with an explicit record that risk tolerance and risk appetite has been assessed and accepted by the relevant executive level committee
 - the maturity of the organisation's capability to manage security risks, and the strategies and actions required to implement effective security risk management
 - how the organisation will maintain a positive risk culture
 - the legal and regulatory obligations of your organisation.
- Identify, implement and monitor the effectiveness of risk mitigation controls in line with the cyber security risk assessment and BYOD policy.

5.2. Refer to [Attachment A](#) for a list of recommended technical and non-technical risk controls Victorian Government Chief Information Security Officer developed to support public service bodies and public entities in implementing the policy guidance and support consistency in organisations' risk management approaches.

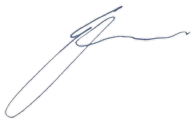
6. Contact

6.1. For further information about these guidelines, please contact the Department of Government Services Cyber Security Branch through cyber.risk@dpc.gov.au.

Emma Cassar

ACTING SECRETARY, DEPARTMENT OF PREMIER AND CABINET

Compliance note: Under section 36A(3) of the Public Administration Act 2004, if a public service body or a public entity to which guidelines have been issued operates, or intends to operate, in a manner that is inconsistent with those guidelines, the relevant public service body Head or public entity Head must provide written reasons for doing so to the Secretary, Department of Premier and Cabinet.



7 July 2023

Attachment A: Risk Controls Recommended by the Victorian Government Chief Information Security Officer

Context

The following advice is provided by the Victorian Government Chief Information Security Officer. It details the recommended controls for managing the risks associated with the use of personal devices to access official systems and data, also known as bring-your-own-device (BYOD) practices.

The recommended controls have been identified from review of existing standards and frameworks in use across both the Commonwealth and Victorian Government, including the Information Security Manual (ISM).

Additional information about implementation methods can be found in the referenced materials.

How to interpret this advice

This advice recommends risk controls against each of the Business Impact Levels defined by the Victorian Protective Data Security Framework.

Victorian Government organisations should consider the Business Impact Level(s) relevant to employees, or cohorts of employees in their organisation, to assist with determining the risk controls that should be applied.

Organisations may also select risk controls relating to the highest relevant Business Impact Level, for application to all employees, if necessary.

Recommended Risk Controls

Recommended General Controls

In addition to applying the enabling controls detailed in the Victorian Protective Data Security Standards and other relevant frameworks, it is recommended that all organisations that allow BYOD practices provide employees with training on:

- cyber security risks and mitigation strategies
- the safe use of social media and messaging applications

Recommended Technical Controls

For organisations that permit employees to use personal devices to access 'UNOFFICIAL' information -

For organisations that permit employees to use personal devices to access 'UNOFFICIAL' information (BIL 0)

Apply the recommended general controls.

For organisations that permit employees to use personal devices to access BIL 1 - 'OFFICIAL' and BIL 2 - 'OFFICIAL: Sensitive' information

Control ID	Control Description
------------	---------------------

ISM-1297 r4	Legal advice is sought prior to allowing privately-owned mobile devices to access systems or data.
ISM-1082 r3	A mobile device usage policy is developed, implemented and maintained.
ISM-1195 r1*	A Mobile Device Management Solution is used to ensure security policy is applied to all devices. <i>*Note: Agencies may consider the use of Mobile Application Management tools to supplement or meet the intention of this control</i>
ISM-1085 r4	Mobile devices encrypt all sensitive or classified data communicated over public network infrastructure.
ISM-0864 r4	Mobile devices prevent personnel from disabling or modifying security functionality once provisioned.
ISM-1366 r2	Security updates are applied to mobile devices as soon as they become available.
ISM-0705 r4	When accessing an organisation's network via a VPN connection, split tunnelling is disabled.
ISM-0240 r7	Paging, Multimedia Message Service, Short Message Service and messaging apps are not used to communicate sensitive or classified data.
ISM-1555 r1	Before travelling overseas with mobile devices, personnel take the following actions: <ul style="list-style-type: none">• record all details of the mobile devices being taken, such as product types, serial numbers and International Mobile Equipment Identity (IMEI) numbers• update all operating systems and applications• remove all non-essential accounts, applications and data• apply security configuration settings, such as lock screens• configure remote locate and wipe functionality• enable encryption, including for any removable media• backup all important data and configuration settings.

For organisations that permit employees to use personal devices to access information up to and including 'PROTECTED' (BIL 3)

Control	Control Description
Implementation of recommended general controls and recommended controls from BIL 1 – OFFICIAL and BIL 2 – OFFICIAL: Sensitive	
ISM-0863 r4	Mobile devices prevent personnel from installing or uninstalling non-approved applications once provisioned.
VPDSS-E2.090	The organisation manages the secure disposal (Archiving / Destruction) of public sector information in accordance with its security value.
ISM-0871 r3	Mobile devices are kept under continual direct supervision when being actively used.
ISM-0870 r3	Mobile devices are carried or stored in a secured state when not being actively used.
ISM-0866 r5	Sensitive or classified data is not viewed or communicated in public locations unless care is taken to reduce the chance of the screen of a mobile device being observed.

For organisations that permit employees to use personal devices to access information up to and including 'SECRET' (BIL 4)

Control	Control Description
ISM-0687 r9	Mobile devices do not store or communicate SECRET or TOP SECRET data until approved for use by ASD. In the event a mobile device is required to store or communicate SECRET or TOP SECRET data, refer to the ACSC's guidance for enterprise mobility .