Administrative Guideline

Direction on the use of DeepSeek Products, Applications and Web Services

Number: 2025/1

Issue: 1.0

dpc.vic.gov.au

VICTORIA State Government | Premier and Cabinet

Acknowledgement of Country

The Victorian Government acknowledges Aboriginal and Torres Strait Islander people as the Traditional Custodians of Country.

We respectfully acknowledge all First Peoples of Victoria and celebrate their enduring connection to land, skies and waters. We thank First People for their care of Country and contributions to Victorian communities. We honour and pay our respects to First Peoples' Elders past and present.

Accessibility

To receive this document in an alternative format, phone **03 9651 5111**, email **vicgov.ciso@dpc.vic.gov.au**, or contact National Relay Service on **1800 555 660** if required. HTML format is available at https://www.vic.gov.au/direction-use-deepseek-products-applications-and-web-services.

For languages other than English, please call the Translating and Interpreting Service National hotline 131 450.

Authorisation

Issued by the Secretary, Department of Premier and Cabinet, under section 36A(1) of the *Public Administration Act 2004*.

JEREMI MOULE

SECRETARY, DEPARTMENT OF PREMIER AND CABINET

12 February 2025

Compliance

Under section 36A(3) of the *Public Administration Act 2004*, if a public service body or a public entity to which the guideline has been issued operates, or intends to operate, in a manner that is inconsistent with this guideline, 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.

Number: 2025/1

Issue: 1.0

Issued by the Secretary, Department of Premier and Cabinet (DPC) in February 2025 and is applicable from date of issue.

These guidelines are subject to periodic amendments. DPC will provide notifications when an update has taken place.

For the latest version please visit: https://www.vic.gov.au/direction-use-deepseek-products-applications-and-web-services.

Contents

Direction on the use of DeepSeek Products, Applications and Web Services

Introduction

Protecting Victorian Government systems and data is essential in creating a cyber safe Victoria and continuing to deliver safe and reliable government services.

This guideline provides direction following the release of **PSPF Direction 001-2025** by the Commonwealth Government's Department of Home Affairs determining that the use of DeepSeek products, applications and web services (*collectively* DeepSeek Products) poses an unacceptable level of security risk to the Commonwealth Government.

For the purposes of this guideline DeepSeek Products means all products, applications, solutions, websites and web services supplied directly or indirectly by DeepSeek or any of its predecessor, successor, parent, subsidiary, or affiliate companies. This does not include open-sourced Large Language Models (LLM) where the entire codebase is available for inspection, the model is deployed locally on a government system, and appropriate mitigations are in place.

This guideline complements the *Administrative Guideline for the safe and responsible use of Generative AI in the Victorian Public Sector* (the Generative AI Guideline) and the *Administrative Guidelines on Improving the Cyber Security of Victorian Government systems and data (the Cyber Security Guidelines)*.

Purpose

This guideline sets out the expectations for public service bodies and public entities to:

- prevent installation and remove existing instances of the DeepSeek Products on government systems and devices unless a legitimate business use reason is approved
- review its bring-your-own-device (BYOD) policy (where BYOD practices are supported) in alignment with this guideline and the requirements outlined in the Cyber Security Guidelines
- identify, implement and monitor the effectiveness of the restrictions on DeepSeek Products and the existing BYOD policy with its associated controls.

Application and commencement

This guideline applies to all public service bodies and public entities, as defined by the *Public Administration Act 2004*. Departments are asked to support communication of the guideline to relevant portfolio entities.

Public service bodies and public entities are expected to manage the requirements of this guideline with their employees, contractors, consultants, volunteers, vendors and any other parties engaged directly or indirectly who have access to Victorian Government owned networks, data or devices.

Certain bodies are not bound by this guideline, 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 this guideline and consider whether it would be appropriate to act consistently.

This guideline commences on the date it is issued.

Public service bodies and public entities should take the necessary steps to ensure they adhere to the guideline as soon as practicable.

Under section 36A(3) of the *Public Administration Act 2004*, if a public service body or a public entity to which the guideline has been issued operates, or intends to operate, in a manner that is inconsistent with this guideline, 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.

The use of DeepSeek Products

Public service bodies and public entities must prevent installation and remove existing instances of DeepSeek Products on government systems and devices unless an approved legitimate business reason exists.

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 DeepSeek Products on government systems and devices.

Where DeepSeek Products need to be removed by employees, volunteers, contractors or consultants on 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 reason exemption

Legitimate business use means a need to install DeepSeek Products on a government system or device to conduct business and/or achieve a work objective of that public service body or public entity.

This guideline limits legitimate business reasons to where the use of a DeepSeek Product is necessary for the carrying out of law enforcement and regulatory functions, including compliance and enforcement functions.

Where a legitimate business reason exemption exists, DeepSeek Products should only be installed after adequate risk and security assessments have been completed, mitigation strategies are implemented, and necessary approval is provided by the public service body head, public entity head or their delegate.

The relevant public service body head or public entity head is to approve any exemption in accordance with this guideline. The public service body or public entity Chief Security Officer (or equivalent) is responsible for ensuring that, at a minimum, the following mitigations are in place prior to providing access to a DeepSeek Product on a government system or device:

- The obligation to adhere to the Generative AI Guideline is communicated to users of the DeepSeek mobile application and web front end, specifically ensuring that only publicly-available information is inputted into the tool.
- DeepSeek Products are installed and accessed only on a separate government issued standalone device without access to services that process or have access to official or classified information.
- The separate, standalone device is appropriately stored and secured when not in use. This includes isolation of these devices from sensitive conversations and information.
- Only a generic email address (for example, a group mailbox) or an otherwise Chief Security Officer (or equivalent) approved email account is used to access DeepSeek products.

- Multifactor authentication (where available) and unique passphrases are used for each account related to a DeepSeek Product.
- Devices associated with DeepSeek Products are using the latest available operating systems to control individual mobile application permissions.
- Regularly checking for, and updating, the application to ensure the latest version is used, unless a specific version is required for the legitimate business use reason.
- Only installing DeepSeek Products for mobile devices from trusted stores such as Microsoft Store, Google Play Store and the Apple App Store.
- Only authorised users have access to government systems or devices with DeepSeek products installed and access is immediately revoked when there is no longer a requirement for that access.
- An appropriately qualified person regularly reviews the terms and conditions of use or installation for DeepSeek Products, as well as application permissions with each update, to ensure appropriate risk management controls can be put in place or adjusted as required.
- DeepSeek Products are deleted from systems and devices when they are no longer required.

The use of personal mobile devices to access official systems and data

Public service bodies and public entities are to apply **Section 5** of Cyber Security Guidelines which outlines requirements for organisations that support employees to use a personal device to access official systems, networks and data, including (but not limited to) work-related emails, messages, documents or corporate applications.

Further, as per the Generative AI Guideline, public service bodies and public entities are to provide training on Generative AI tools. This should include information on the benefits and risks of Generative AI and on their responsibilities related to the use of Generative AI tools for official work purposes.

Contact

For further information about this guideline, please contact the Department of Government Services Cyber Security Data and Digital Resilience Division through vicgov.ciso@dpc.vic.gov.au.

dpc.vic.gov.au

VICTORIA State Government | Premier and Cabinet