



Australian Government

Department of Home Affairs
Protective Security Policy Framework

OFFICIAL

PSPF Direction 001-2025

DeepSeek Products, Applications and Web Services

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 technical authority entities, the Secretary of the Department of Home Affairs may issue a Direction to accountable authorities to manage a protective security risk to the Commonwealth.

The Accountable Authority of each entity must adhere to any Direction issued.

PSPF Direction 001-2025 requires Australian Government entities¹ to prevent the access, use or installation of DeepSeek products, applications and web services² and where found remove all existing instances of DeepSeek products, applications and web services from all Australian Government systems and devices³.

After considering threat and risk analysis, I have determined that the use of DeepSeek products, applications and web services poses an unacceptable level of security risk to the Australian Government.

Entities must manage the risks arising from DeepSeek's extensive collection of data and exposure of that data to extrajudicial directions from a foreign government that conflict with Australian law.

As of 4 February 2025, all non-corporate Commonwealth entities **must**:

1. Identify and remove all existing instances of DeepSeek products, applications and web services on all Australian Government systems and mobile devices.
2. Prevent the access, use or installation of DeepSeek products, applications and web services on all Australian Government systems and mobile devices.
3. Report completion of above requirements to the Department of Home Affairs' Commonwealth Security Policy Branch at PSPF@homeaffairs.gov.au.

¹ For the purposes of this Direction, 'Australian Government entities' refers to all *non-corporate Commonwealth entities that are subject to the Public Governance, Performance and Accountability Act 2013 (PGPA Act)*.

² 'Products, applications and web services' constitutes *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 as outlined in Policy Explanation Note 001-25 – DeepSeek Products, Applications and Web Services.*

³ 'Devices' constitutes *'Government-issued mobile devices' and 'authorised non-government devices', as defined in the PSPF, which includes all mobile phones, handheld computers, tablets, laptops and personal digital assistants.*

OFFICIAL

OFFICIAL

The Accountable Authority may seek an exemption for a legitimate business reason, limited to national security and regulatory functions, for the use of DeepSeek products, applications and web services² on government devices and must ensure that appropriate mitigations are in place.

Legitimate business reason is a need to install or access the DeepSeek products, applications or web services on a government system or mobile device to conduct business and/or achieve a work objective of an entity. A legitimate business reason must be time limited, follow all mitigations outlined in Policy Explanatory Note 001-25 and be limited to:

- where the use is necessary for the carrying out of national security or regulatory functions, including compliance and law enforcement functions.

Further information about DeepSeek products, applications and web services; similar offerings; and appropriate mitigations for legitimate business use is detailed in Policy Explanatory Note 001-25 – DeepSeek Products, Applications and web services.

For further information, contact PSPF@homeaffairs.gov.au or 02 5127 9999.

Stephanie Foster

Stephanie Foster PSM

Secretary

Department of Home Affairs

4 February 2025