

SACSF Ruling 4 – Use of DeepSeek in the South Australian Government

SACSF/R4.0

Government Ruling on Cyber Security

Purpose

This Ruling provides a direction to South Australian (SA) Government agencies under the South Australian Cyber Security Framework (SACSF) on the access, use, and installation of DeepSeek products, applications and web services¹.

The Australian Government has determined that the use of DeepSeek products, applications and web services pose an unacceptable level of security risk.

Scope

The SACSF applies to SA public sector agencies (as defined in section 3(1) of the [Public Sector Act 2009](#)) and to any other person or organisation that is generally subject to the direction of a Minister of the Crown; all of which are referred to in this Ruling as “Agencies”.

A SACSF Ruling is a mandatory application of SACSF Policy.

This Ruling does not impact the use of DeepSeek on personal devices. However, agencies that accept the risks of personal devices being used 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 DeepSeek as part of this policy position and should implement technical controls to mitigate the risks associated with the installation of DeepSeek on personal devices.

Ruling

Agencies must prevent the access, use or installation of DeepSeek products, applications and web services and, where found, remove all existing instances of DeepSeek products, applications and web services from all SA Government systems and devices²:

Agencies 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.

¹ ‘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.

² ‘Devices’ constitutes government owned mobile devices, which includes all mobile phones, handheld computers, tablets, laptops and personal digital assistants.

As of 5 February 2025, all agencies must:

1. Identify and remove all existing instances of DeepSeek products, applications and web services on all SA Government systems and mobile devices.
2. Implement technical controls to prevent the access, use or installation of DeepSeek products, applications and web services on all SA Government systems and devices.
3. Instruct agency staff that they must not use DeepSeek for any government work purposes nor post any government information into DeepSeek applications or web services.

Exemptions:

- 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 services on SA Government devices and must ensure that appropriate mitigations are in place.
- A legitimate business reason is a need to install or access the DeepSeek products, applications or web services on an SA Government system or mobile device to conduct business and/or achieve a work objective of an agency.
- A legitimate business reason must be time limited, include mitigations, 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.
- Exemptions must be sought through the [Office of the Chief Information Officer exemption process](#).

Aboriginal Impact Statement

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

Roles and responsibilities

Position title or unit/team	Listed responsibilities
Accountable Authority	Accountable for the effective implementation of, and compliance with this Ruling within their agency.
Agency Security Executives	Responsible for ensuring that the Ruling is implemented within the agency and that business processes support the Ruling requirements.
Agency IT Security Advisor	Responsible for providing advice on application of this Ruling within the agency environment.

Definitions

Term	Definition
Accountable Authority	The person or group of persons responsible for, and with control over, the agency's operations (e.g. Chief Executive, Commissioner).
DeepSeek products, applications and web services	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.
Devices	SA Government owned mobile devices, which includes all mobile phones, handheld computers, tablets, laptops, and personal digital assistants.

Related Documents

- [PC030 Protective Security in the Government of South Australia](#)
- [South Australian Protective Security Framework](#)
- [South Australian Cyber Security Framework](#)
- [Protective Security Policy Framework Direction 001-2025 on DeepSeek Products, Applications and Web Services](#)

Document Control

Approved by	CIO Steering Committee	Version	V1.1
Approved date	13 October 2026	Next review date	October 2027
Original date of approval	5 February 2025	Compliance	Mandatory
Contact:	Cyber Security Directorate, Office of the Chief Information Officer		
Contact email	cybersecurity@sa.gov.au		

Licence



With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a [Creative Commons Attribution \(CC BY\) 4.0 Licence](#). To attribute this material, cite the Office of the Chief Information Officer, Department of Treasury and Finance, Government of South Australia, 2026.