Direction 1-2025

Direction on the use of DeepSeek

Resilience and Recovery Tasmania
Department of Premier and Cabinet

Tasmanian Government

Direction on the use of DeepSeek

Tasmania's Protective Security Policy Framework (TAS-PSPF) currently applies to Tasmanian Government agencies and their subsidiaries, per section 1.3 of the framework.

Under the **TAS-PSPF policy: Establish security governance (GOVSEC-1)**, Accountable Authorities must action their roles and responsibilities, which includes adhering to any direction issued under the TAS-PSPF.

This direction (Direction 1-2025) addresses the use of DeepSeek on Tasmanian Government systems and devices. Informed by national intelligence and security advice, I have determined that the use of DeepSeek products, applications and web services poses an unacceptable level of security risk to the Tasmanian Government. This is due to DeepSeek's extensive collection of data and exposure of that data to extrajudicial directions from a foreign government that conflict with Australian law.

Required action: Prohibit the use of DeepSeek

The Accountable Authority must:

- prevent the access, use or installation of DeepSeek products, applications and web services[1] on all Tasmanian Government systems[2] and devices[3]; and
- ensure removal of all existing instances of DeepSeek products, applications or web services from Tasmanian Government devices and systems.

This includes devices issued to all people within your agency[4].

The Accountable Authority must report completion of these requirements to Resilience and Recovery Tasmania in the Department of Premier and Cabinet via taspspf@dpac.tas.gov.au.

[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.

[2] 'Systems' are a related set of hardware, software and supporting infrastructure used for the processing, storage or communication of data and the governance framework in which it operates.

[3] 'Devices' includes mobile phones, computers, laptops, tablets and personal digital assistants.

[4] Per the TAS-PSPF, 'people' is defined as:

> *Employees and contractors, including secondees and any service providers that an agency engages. It also includes anyone who is given access to Tasmanian Government assets.*

The Accountable Authority must ensure the known security risks are managed by implementing appropriate mitigations when authorising the use of DeepSeek.

This direction is to be actioned as soon as practicable.

Further information regarding DeepSeek products, applications and web services, and similar offerings, is detailed in the Australian Government's *Policy Explanatory Note 001-25 – DeepSeek Products, Applications and Web Services*, which will be available to the Tasmanian Government on request.

For more information and support on implementing this Direction, please contact your Chief Information Officer in the first instance, or Digital Strategy and Services in the Department of Premier and Cabinet via cybersecurity@dpac.tas.gov.au.

For advice on the TAS-PSPF, please contact your Agency Security Advisor or Resilience and Recovery Tasmania via taspspf@dpac.tas.gov.au.

Authorisation

I, Jeremy Rockliff, the Premier of Tasmania and the authority of the TAS-PSPF, require Accountable Authorities to adhere to this direction issued on the 6 day of February 2025.

Issued and authorised by:

Jeremy Rockliff MP
Premier

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7979

Email:
taspspf@dpac.tas.gov.au