Australian Government
Department of Home Affairs
Protective Security Policy Framework

POLICY ADVISORY 001-2025

OFFICIAL Information Use with Generative Artificial Intelligence

Generative AI presents exciting opportunities to improve how government entities manage and use OFFICIAL information in their daily operations.

This Policy Advisory supports the safe and confident adoption of generative artificial intelligence (AI) by offering clear, whole-of-government guidance under the Protective Security Policy Framework (PSPF). It confirms that OFFICIAL information—including data used for business and service delivery—can be used with generative AI.

By aligning with the principles in this advisory, entities can take advantage of trusted AI platforms from Australian and foreign companies, ensure responsible staff training, and follow streamlined approval processes provided by the Department of Home Affairs. These steps help organisations unlock the benefits of generative AI—such as increased efficiency and innovation—while maintaining secure and responsible practices.

Policy Advisory

This Policy Advisory for the PSPF provides official whole-of-government advice for the use of OFFICIAL information with generative AI technologies.

OFFICIAL information, including information created for business operations and services, can be used[1] **with generative AI technologies**.

Access to generative AI technologies must be assessed in accordance with existing responsibilities under the PSPF.

Adopting the following principles ensures entities have appropriately considered and managed data security risks when incorporating generative AI into business operations.

[1] 'Use' of generative AI products includes software hosted on internal technology systems / mobile devices or provided via outsourced service providers, and web-based products, including websites such as ChatGPT.com, accessed through web browsers or cloud service providers.

Entities must:

1. Only provide access to generative AI products hosted on Hosting Certification Framework providers, OpenAI or Anthropic; or have undergone a Foreign Ownership, Control, or Influence (FOCI) risk assessment.[2]
2. Ensure staff training includes guidance on handling security classified information when using generative AI.[3]
3. Follow the existing PSPF technology authorisation process[4] and consider relevant Australian Signals Directorate Guidance when approving access to generative AI tools for use with OFFICIAL information.[5]

Adopting the principles outlined in this Policy Advisory in accordance with the PSPF gives entities confidence in approving the use of generative AI for OFFICIAL information, while ensuring safe and responsible practices.

Version	**FINAL Version** 1.0, 07/10/2025
Intended Audience	Accountable Authorities Chief Security Officers Chief Information Security Officers Procurement Officers
Contact	Commonwealth Security Policy Branch, Department of Home Affairs PSPF@homeaffairs.gov.au

[2] Entities providing access to generative AI products certified under the Hosting Certification Framework, OpenAI and Anthropic, do not require additional FOCI assessment to the assurance provided by the Department of Home Affairs. All other providers must be assessed in accordance with PSPF Direction 001-2024 before allowing access.

[3] Details on how to structure training on responsible AI use can be found via Digital Transformation Agency's Guidance for staff training on AI.

[4] As outlined in **PSPF Requirement 0086** *The Authorising Officer authorises each technology system to operate based on the acceptance of the residual security risks associated with its operation before that system processes, stores or communicates government information or data*, **PSPF Requirement 0087** *Decisions to authorise (or reauthorise) a new technology system or make changes to an existing technology system are based on the Information Security Manual's risk-based approach to cyber security*; and **PSPF Requirement 0088** *The technology system is authorised to the highest security classification of the information and data it will process, store or communicate*

[5] For technical guidance refer to the Australian Signals Directorate's (ASD's) Engaging with artificial intelligence guidance, ASD's latest version of the Information Security Manual and ASD's Zero Trust Modern Defensible Architecture Principles.