PSPF Direction 004-2025

Commonwealth Technology Management

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 004-2025 requires Australian Government entities to adhere to the Commonwealth Technology Standard which provides guidance on products, applications and web services for use on Australian Government systems[1] and devices[2].

Further information about the Commonwealth Technology Standard is detailed in Policy Explanatory Note 005-2025 – Commonwealth Technology Management.

After considering threat and risk analysis, I have determined that further guidance is required to respond to the growing use of products, applications and web services within Australian Government entities that pose an unacceptable level of security risk to Australian Government networks and data arising from threats of foreign interference, espionage and sabotage.

The Commonwealth Technology Standard provides guidance on products, applications and web services for use within Australian Government entities.

From 31 October 2025, all non-corporate Commonwealth entities **must**:

1. Identify and remove all existing instances of products, applications and web services identified on the *Deny List* of the Commonwealth Technology Standard.
2. Prevent the installation of any new products, applications and web services identified on the *Deny List* of the Commonwealth Technology Standard.
3. Report completion of above requirements to the Department of Home Affairs' Commonwealth Security Policy Branch at PSPF@homeaffairs.gov.au, as identified in the *Deny List*.

From 2 February 2026, all non-corporate Commonwealth entities **must**:

1. Implement a policy to consider sharing risk assessments through the Department of Home Affairs Centralised Risk Sharing Capability.
2. Implement a process when undertaking technology system authorisation that considers applications and web services identified on the *Applications Policy* of the Commonwealth Technology Standard.
3. Report completion of above requirements to the Department of Home Affairs' Commonwealth Security Policy Branch at PSPF@homeaffairs.gov.au,as identified in the *Applications Policy*.

---

[1] 'Systems' constitutes *the related set of hardware (including but not limited to desktop computers), software and supporting infrastructure used for the processing, storage or communication of information/data and the governance framework in which it operates.*

[2] '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.*

The Accountable Authority may seek an exemption for a legitimate business reason for the use of products, applications and web services identified on the Commonwealth Technology Standard *Deny List*, on Australian Government systems and devices and must ensure that appropriate mitigations are in place.

Legitimate business reason is a need to install or access the products, applications and web services identified on the Commonwealth Technology Standard *Deny List* on an Australian 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 and follow all mitigations outlined in Policy Explanatory Note 005-2025.

A legitimate business reason would include:

- where the application is necessary for the carrying out of regulatory functions including national security, compliance and law enforcement,
- where an entity requires research to be conducted or communications to be sent to assist with a work objective (for example, countering mis- or dis-information), or
- where an entity must use the application to reach key audiences to undertake marketing or public relations activity on behalf of the entity.

The Centralised Risk Sharing Capability for the Commonwealth will be made available by 2 February 2026.

Further information about the Commonwealth Technology Standard and appropriate mitigations for legitimate business use is detailed in Policy Explanatory Note 005-2025 – Commonwealth Technology Management.

For further information, contact PSPF@homeaffairs.gov.au.

Stephanie Foster

Stephanie Foster PSM
Secretary
Department of Home Affairs
22 October 2025