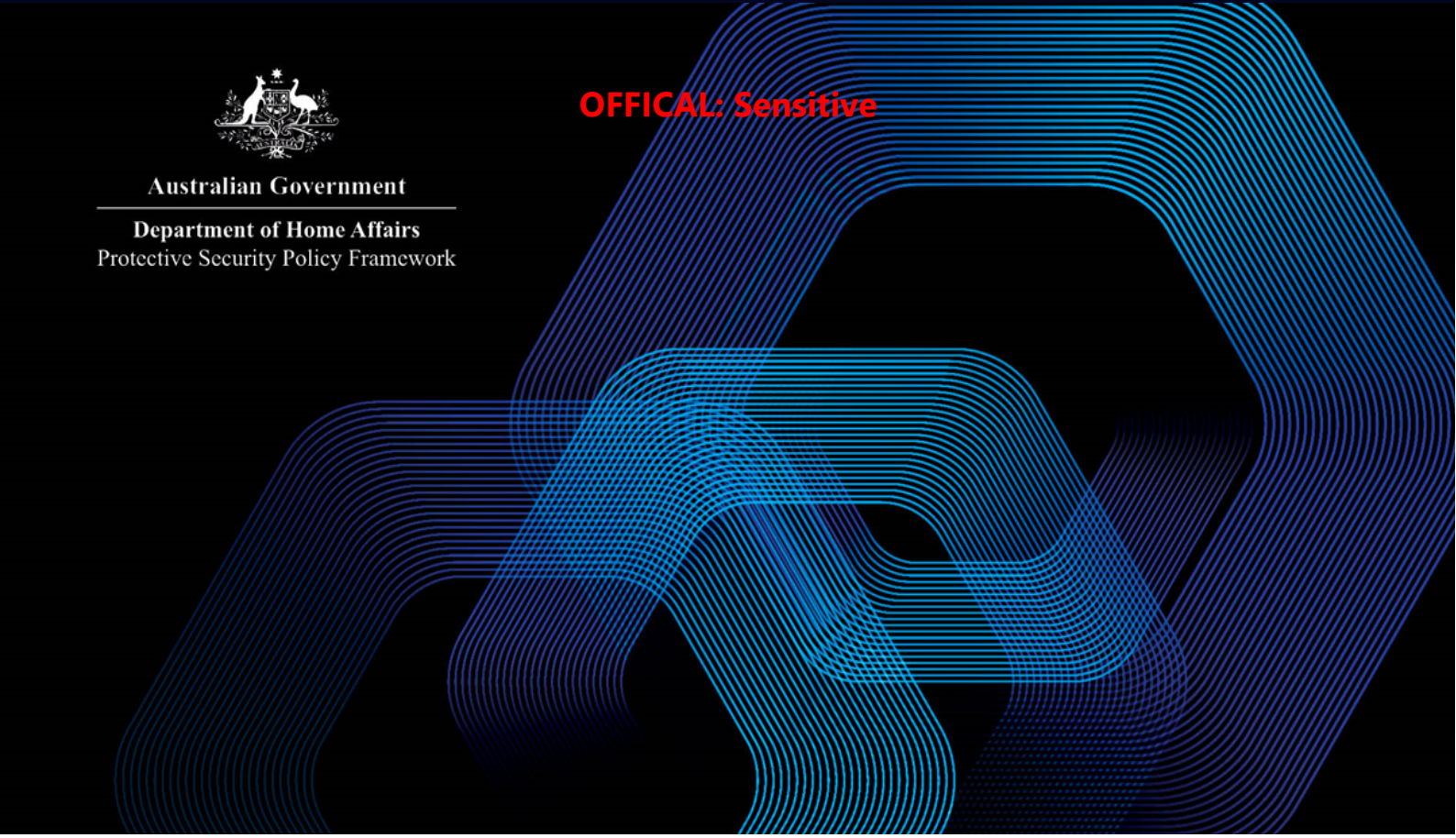


Australian Government Commonwealth Technology Standard

Table of Contents

Purpose 3

Audience and Applicability 4

Document Control 4

1. Commonwealth Technology Management 5

1.1. Governance Procedures 5

1.2. Application Control 6

1.2.1. Implementing Application Control 6

1.2.2. Implementing Application Control for Mobile Devices 9

1.3. Web Services Control 9

2. CTS Applications Policy and Deny List 10

2.1. Security Classification of the *Applications Policy* and *Deny List* 10

2.2. Applications Policy and Deny List Definitions 10

2.2.1. Permitted Use Case 11

2.2.2. Application and Web Service Categories 11

2.3. Deny List Additions 12

2.3.1. Implementation and Communication 12

2.3.2. Access to the *Deny List* for Entities Without SECRET Systems 13

2.3.3. Communications Mechanisms for Additions 13

2.4. Centralised Risk Sharing Capability 13

3. Risk Assessment 14

3.1. Foreign Ownership, Control or Influence 15

4. Evaluation and Exemption Process 15

4.1. Evaluation Process to be added to CTS Applications Policy 15

4.2. Exemption Process for a Legitimate Business Reason 15

4.2.1. Exemption Process 16

5. Glossary 18

5.1. Glossary of Abbreviations 18

5.2. Glossary of Terms 18

ANNEX A – Commonwealth Technology Standard Applications Policy 20

ANNEX B – Commonwealth Technology Standard Deny List 21

ANNEX C – Applications Policy Evaluation Request Form 22

ANNEX D – Deny List Exemption Request Form 23

Purpose

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

The Protective Security Policy Framework (PSPF) requires that all products, applications, and web services are approved to be installed, accessed, or used on Australian Government technology systems. This includes devices that access, process, store or communicate security classified information or data.

While not exhaustive, the CTS supports entities by providing a repeatable process for the management of applications in the modern technology environment and eliminates duplicative and inconsistent effort in risk assessment and decision-making across the Australian Government.

Requirement 0221 | TECH | All entities | 01 July 2026

The Australian Government Commonwealth Technology Standard and its annexes are applied when authorising technology systems to operate up to SECRET.

Requirement 0222 | TECH | All entities | 01 July 2026

A policy that considers sharing risk assessments of products, applications and web services to the Department of Home Affairs' Centralised Risk Sharing Capability is established.

The CTS sets out the:

- Commonwealth Technology Management processes outlined in PSPF Release 2026 (Section 13.5)
- application control process required by the PSPF and the Australia Signals Directorate's (ASD) Strategies to Mitigate Cyber Security Incidents
- *Applications Policy* and *Deny List* of products, applications and web services
- risk assessment approach for entities considering products, applications and web services not included on either the *Applications Policy* or *Deny List*
- evaluation process, and
- exemption process.

The CTS reduces the administrative burden of issuing multiple PSPF Directions on products, applications and web services that present an unacceptable risk to the Australian Government's technology estate. PSPF Directions may still be issued when specific or urgent threats have been identified that require immediate remediation.

The CTS will be updated as required and reviewed annually as part of the PSPF annual release cycle. Amendments to the CTS will be approved by the Department of Home Affairs in consultation with the relevant Technical Authority Entities (TAEs).

The *Applications Policy* will be managed and informed by the Department of Home Affairs Centralised Risk Sharing Capability. New applications or technologies will only be included on the *Deny List* by the Government Security Committee or the Protective Security Board on the advice of a:

- Technical Authority Entity
- Risk assessment from the Department of Home Affairs, or
- Technology Vendor Review Framework recommendation.

Audience and Applicability

The CTS applies to all non-corporate Commonwealth entities (entities), as defined by the *Public Governance, Performance and Accountability Act 2013* and listed on the Department of Finance's Flipchart of Commonwealth entities and companies.

The CTS **does not** apply to technology systems, including mobile devices, authorised to process, store, or communicate information at the TOP SECRET security classification.

Document Control

This document is maintained by the Department of Home Affairs and forms part of the Australian Government Protective Security Policy Framework (PSPF).

Contact the Protective Security Policy Section in the Department of Home Affairs via email at PSPF@homeaffairs.gov.au for changes or advice.

No.	Description	Date
1.0	Initial release.	2025-12-19
2.0	Update under PSPF Release 2026 – applicability changed from PSPF Direction 004-2025 to PSPF Requirements 0221 and 0222. GSC agreed to implementation and guidance for *Deny List* additions.	2026-07-01

1. Commonwealth Technology Management

PSPF Requirement 0221 mandates that the Australian Government Commonwealth Technology Standard and its annexes are applied when authorising technology systems to operate up to SECRET.

PSPF Release 2026 Section 13.3 – Technology System Authorisation requires that all technology systems are authorised to operate or be used in the entity. The authorisation process ensures that an appropriate level of security is being applied to the technology system and that residual security risks have been accepted by the relevant authority.

PSPF Release 2026 Section 13.4 – Applications Management mandates that all applications require approval to be installed or used on resources that access Australian Government technology systems or data. The application management process ensures applications are managed from procurement decisions, deployment of the application, maintenance through to decommission and involves both governance procedures and application control.

Technology management, including authorisation of technology systems and the CTS, forms part of broader technology lifecycle management. PSPF Release 2026 Chapter 13 – Technology Lifecycle Management outlines that entities must manage all technology systems across designing, developing, planning, procurement, deployment and maintenance through to retirement.

PSPF Requirement 0085 mandates the ISM controls and cyber security guidelines are applied on a risk-based approach. This risk-based approach comprises the following six steps:

- Step 1 – Define the Technology System
- Step 2 – Select security controls
- Step 3 – Implement security controls
- Step 4 – Assess security controls
- Step 5 – Authorise the technology system
- Step 6 – Monitor the technology system

Refer to the PSPF Guidelines Section 13.1.2 for further information.

1.1. Governance Procedures

Technology lifecycle management governance ensures that products, applications and web services that are installed, accessed or used on resources that access Australian Government technology systems or devices that access, process, store or communicate security classified information or data are appropriately secure.

Products, applications and web services form part of an entity's technology systems.

PSPF Release 2026 Section 13.3 – Technology System Authorisation requires that all technology systems are authorised to operate or be used in the entity. The authorisation process ensures that an appropriate level of security is being applied to the technology system and that residual security risks have been accepted by the relevant authority.

PSPF Release 2026 (Table 21) details the Authorising Officer and Security Assessor for each technology.

PSPF Requirement 0089 requires that a register of the entity's authorised technology systems is developed, implemented and maintained and includes the name and position of the Authorising Officer, system owner, date of authorisation, and any decisions to accept residual security risks.

1.2. Application Control

The Australian Signals Directorate's (ASD) Strategies to Mitigate Cyber Security Incidents helps entities protect against various cyber threats with the most effective of these mitigation strategies being the Essential Eight. One such mitigation strategy under the Essential Eight is Application Control.

PSPF Requirement 0103 requires that entities implement an application control mitigation strategy to Maturity Level Two under ASD's Essential Eight Maturity Model.

Malicious code (malware) often aims to exploit vulnerabilities in existing applications and does not need to be installed on workstations or servers to be successful. If appropriately configured, application control helps to prevent undesired execution of software regardless of whether the software was downloaded from a website, clicked on as an email attachment or introduced via CD/DVD/USB removable storage media.

See PSPF Release 2026 Section 14.2.5 – Application Control for further details.

Entities should consider categorising products, applications and web services as part of their application and web service control strategies. Refer to CTS Section 2.2.2 – Application and Web Service Categories for details.

1.2.1. Implementing Application Control

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

The *Applications Policy* is the list of applications and web services that entities **may** use or access without needing to conduct a risk assessment.

The *Applications Policy* is **best-practice** and **voluntary**, and is currently restricted to the following categories of applications and web services which represent the most significant risk to the Australian Government's technology estate, including:

- Social Media,
- Communications,
- Office Productivity Tools, and
- Security Software.

Entities **must** implement a process when undertaking technology system authorisation that considers applications and web services identified on the *Applications Policy* of the Commonwealth Technology Standard.

The *Deny List* identifies products, applications and web services that entities **must not** install or access, except in the case of a legitimate business reason, and is **mandatory**. It requires entities to:

- identify and remove all existing instances of applications and web services identified on the *Deny List*, and
- prevent the installation of any new applications and web services identified on the *Deny List*.

ASD's Implementing Application Control provides technical guidance on employing application control strategies. These strategies include the following high-level steps:

- identifying approved applications utilising the CTS *Applications Policy* and *Deny List,*
- developing application control rules to ensure only approved applications are allowed to execute,
- maintaining application control rules using a change management program, and

- validating application control rules and their implementation on an annual or more frequent basis.

When determining how to enforce application control, the following methods are considered suitable if implemented correctly:

- cryptographic hash rules,
- publisher certificate rules (combining both publisher names and product names), and
- path rules (ensuring file system permissions are configured to prevent unauthorised modification of folder and file permissions, folder contents and individual files).

For further guidance on application control refer to ASD's Strategies to Mitigate Cyber Security Incidents.

For technical guidance on content filtering refer to ASD's Guidelines for Gateways - Content Filtering.

1.2.1.1. Identifying Products, Applications and Web Services

To identify the use of products, applications and web services entities should consider:

- Checking user browser history – to provide insight on whether users have visited web addresses, domains, and if they have downloaded program files.
- Auditing enterprise logging systems – to identify if users have accessed, downloaded, or installed products, applications, and web services identified on the *Deny List* of the CTS. Event logging systems should be configured to log usage of an entity's internet-facing services including websites visited and programs downloaded and log a history of software installation.
- Managing security tools – software or services used to protect technology systems, information, and data. Examples of security tools include:
  - Antiviruses – generally used to identify malicious files, antivirus scanning can be configured to more broadly identify specific files types. Multiple different scanning engines should be used to increase the likelihood of identifying files.
  - Endpoint management – software that allows entities to manage devices and users from a single piece of software. Endpoint management software can be configured to identify the installation of any software on a computer or device managed by the entity.
  - Mobile device management – software solutions that can manage the administration of mobile devices and allows for logging of the usage of specific websites and software.
- Cyber security functions – can be used to detect the usage of specific products or web services. Cyber security may be performed by dedicated, diverse teams, or may be incorporated into other IT roles, particularly for small entities. Cyber security teams and roles perform numerous functions for identifying usage including:
  - Security Operating Centre (SOC) review – a SOC helps protect an entity's systems and devices and can be used to perform a review of event logs or change management requests.
  - Threat hunting – this is generally used proactively but can be used to search through the entity's networks, endpoints and datasets to identify use of web services or downloaded applications.
- Communicate to staff instructing them to report on if they have installed, accessed, or used products, applications or web services identified on the *Deny List*.

1.2.1.2. Removing Products, Applications and Web Services

Many of the controls and solutions used to identify the use of products, applications and web services can also be used to remove them.

To remove products and applications, entities should consider using:

- Admin accounts for uninstalling – admin accounts, including network domain admins, with sufficient privileges to utilise the in-built tools present on systems and devices.
- Security tools – software or services used to protect technology systems, information, and data. Examples of security tools include:
  - Endpoint Management software – allows entities to manage devices and users from a single piece of software, including remotely uninstalling programs and applications.
  - Mobile device management – software solutions that can manage the administration of mobile devices and allows administrators to uninstall programs and applications.

1.2.1.3. Prevent the Access to Products, Applications and Web Services

PSPF Requirement 0113 mandates that an Australia Government entity's internet-connected technology systems, and the data they process, store or communicate, are protected by a gateway in accordance with the Information Security Manual and the Gateways Policy. A gateway is a data flow control mechanism that plays a vital role in securing a technology system by providing entities with protection at its perimeter.

To prevent access, entities should consider using:

- Web content filtering – to only allow approved types of web content and websites with good reputation ratings, and block access to specific domains and IP addresses.
- Configuring web browsers – using gateway web proxies that block access to specific categories of websites, types of content, and domains, including artificial intelligence (AI).
- Gateways – A gateway is a boundary system that separates different security domains and acts as the first line of defence to provide security capabilities for an organisation and its systems. Gateway solutions provide Australian Government entities with a broad suite of cyber security functionality and capabilities at the boundary of their security domains. Gateways can be configured for blocking, inspecting, filtering and validating actions through Policy Enforcement Points, and can be used to prevent access to products, applications and web services on the Deny List.
  - Requirement 0214 mandates that digital Infrastructure that processes, stores or communicates Australian Government security classified information is protected by a Gateway or Security Service Edge in accordance with the Australian Government Gateways Standard.
  - Refer to ASD's Guidelines on Gateways for further guidance.
- Communicate to staff to inform them that they must not access or use products, applications and web services in support of this Standard.

1.2.1.4. Preventing Installation of Products, Applications and Web Services

PSPF Requirements 0099 to 0106 mandates that entities employ the Australian Signals Directorate's (ASDs) Essential Eight mitigation strategies, and consider the remaining strategies from the Strategies to Mitigate Cyber Security Incidents, to help protect against various cyber threats.

The most relevant strategies of the Essential Eight to prevent installation are:

- Restricting administrative privileges – to prevent the installation of unapproved applications by controlling privileged account access and their associated permissions.
- Application control – to ensure that only approved applications can be executed. Mobile Application Management software provides the same control for mobile devices.

For further guidance on implementing these security controls, refer to ASD's:

- Essential Eight,
- Strategies to Mitigate Cyber Security Incidents, and
- Strategies to Mitigate Cyber Security Incidents – Mitigation Details

1.2.2. Implementing Application Control for Mobile Devices

Application control must apply to all technology systems and devices.

Devices include 'government-issued mobile devices and 'authorised non-government devices', as defined in PSPF Release 2026 Sections 9.3.2 and 9.3.3, which includes all mobile phones, handheld computers, tablets, laptops and personal digital assistants.

Mobile Application Management (MAM) software allows entities to apply similar application control measures identified in Section 1.2 – Application Control for mobile devices. Refer to ASD's Blueprint for Secure Cloud Endpoint Management and Device Management for technical controls relating to Mobile Application Management (MAM) and Mobile Device Management (MDM).

1.2.2.1. Management of Messaging Applications

Entities are recommended to regularly check the member list of applications, products and web services they use, including group chats, to ensure that unauthorised users are not permitted access. Entities should additionally check the 'linked devices' section, and remove any unknown or suspicious contacts or devices, due to the potential for malicious actors to bypass encryption methods. Entities are recommended to secure their applications, products and web services through either a PIN code, biometrics or password, where possible.

1.2.2.2. All Other Mobile Devices

The CTS *Deny List* does not impact the use of products, applications and web services on all other mobile devices that are not owned, issued or authorised by the entity to access, process, store or communicate government security classified information, including personal devices.

Entities that accept the risks of the use of personal devices to access, process, store or communicate government security classified information (i.e. pursuant to remote access arrangements including Bring Your Own Device (BYOD) or equivalent policies), **must**:

- provide access to that data through non-persistent and full remote access solutions that are approved by the Chief Security Officer, Chief Information Security Officer, or their delegate, as opposed to using the native storage and applications on the personal device, and
- provide guidance to all staff that highlights that products, applications and web services identified on the CTS *Deny List* present an unacceptable risk to Australian Government entities arising from extensive collection of user data and exposure to extrajudicial directions from a foreign government that conflicts with Australian law.

Entities cannot restrict the use of products, applications and web services on personal devices, but are recommended to request that personnel remove, do not access, and do not install products, applications and web services identified on the CTS *Deny List* when using BYOD or equivalent policy devices.

1.3. Web Services Control

Web services also present security risks to Australia Government technology systems and information.

Entities **must** ensure that web services listed on the CTS *Deny List* are not used or accessed by personnel. The *Deny List* details the products, applications and web services that are assessed as unsuitable for use within Australian Government entities. Refer to ANNEX B – Commonwealth Technology Standard.

To prevent access, entities should consider using:

- Web content filtering – to only allow approved types of web content and websites with good reputation ratings, and block access to specific domains and IP addresses.
- Configuring web browsers – using gateway web proxies that block access to specific categories of websites, types of content, and domains.
- Communicate to staff to inform them that they must not access or use web services in support of this Standard.

For technical details on recommended mitigation strategies for web services refer to ASD's:

- Strategies to Mitigate Cybersecurity Incidents
- Strategies to Mitigate Cybersecurity Incidents: Mitigation Details
- Guidelines for Gateways.

The Information Security Manual (ISM) also lists controls for mitigation risks in web services, notably:

- ISM Control: ISM-0963; Revision: 7 – Web content filtering is implemented to filter potentially harmful web-based content.

2. CTS Applications Policy and Deny List

The *Applications Policy* is available at Annex A.

The *Deny List* is available at Annex B.

2.1. Security Classification of the *Applications Policy* and *Deny List*

The Commonwealth Technology Standard, including all information identified on both the *Applications Policy* and *Deny List*, is security classified and must be handled in accordance with PSPF Requirement 0062.

Personnel must hold an appropriate security clearance level commensurate with the security classification of the material they will access, in accordance with in accordance with PSPF Release 2026 (Table 25), and must have a genuine need-to-know to access the CTS.

The CTS is security classified OFFICIAL: Sensitive. The Applications Policy and Deny List are security classified SECRET.

The Department of Home Affairs is the originator of the CTS and may, at times, choose to allow certain information on the *Applications Policy* and *Deny List* to be made public. Publication of individual applications, products or webs services identified on either the *Applications Policy* or *Deny List* will require a:

- public PSPF Direction (such as with DeepSeek and Kaspersky)
- decision of the Protective Security Board, or
- Cabinet decision.

2.2. Applications Policy and Deny List Definitions

The CTS *Applications Policy* and *Deny List* are defined below.

Table 1: Commonwealth Technology Standard List Definitions

CTS List Type	Definition	Applicability
Applications Policy	The list of applications and web services that entities **may** use or access, without needing to conduct a risk assessment. The *Applications Policy* acts as an enabler for Commonwealth entities by reducing duplicative effort in the risk assessment process and is based on existing lists in use across government. It is informed by the Centralised Risk Sharing Capability, which will be made available to the Commonwealth. The list is not exhaustive and is best-practice guidance based on the Centralised Risk Sharing Capability operated by the Department of Home Affairs.	**Voluntary (best-practice)**
Deny List	The list of products, applications and web services that entities **must not** install or access, except in the case of a legitimate business reason. The *Deny List* offers the Commonwealth entities a security classified, repeatable, low-risk process for managing increasingly complex application risk. It: • is initially based on existing PSPF Directions, • has been developed in consultation with Technical Authority Entities, and existing policy functions such as the Technology Vendor Review Framework, and • includes an exemption process which will align with previous PSPF Directions. Refer to section 4 – Evaluation and Exemption Process for details on the exemption process.	**Mandatory**

2.2.1. Permitted Use Case

The CTS *Deny List* includes provisions that allow for the permitted use of products, applications and web services included on the list, under specific situations and with stringent requirements.

Entities **must** only install products and applications, or allow access to web services, included on the *Deny List* where they meet the requirements and technical controls included in the **Permitted Use Case** section of the *Deny List.*

The Permitted Use Case is separate from the exemption process, whereby the Accountable Authority of an entity may seek an exemption for use products, applications, and web services on the *Deny List*, for a legitimate business reason. Refer to CTS Section 4 – Evaluation and Exemption Process for details.

2.2.2. Application and Web Service Categories

The CTS *Applications Policy* is currently restricted to four categories of applications and web services, which are defined below.

Table 2: Applications and Web Services Categories

Category	Definition
Social Media	Products, applications and web services that are intended to facilitate the creation, sharing and aggregation of content for consumption by the public or large communities. Examples: Facebook, YouTube, Instagram, WhatsApp, TikTok
Communications	Products, applications and web services that facilitate direct messaging or sharing of information between individual recipients or small groups of recipients. Examples: Signal, WhatsApp, Facebook Messenger

Category	Definition
Office Productivity Tools	Products, applications and web services that are intended to be used to produce, format and adjust the display of information produced as part of day-to-day office work. Examples: • Word processors – Microsoft (MS) Word, Google Docs • Spreadsheet applications – MS Excel, Google Sheets • PDF reader – Adobe Acrobat • Web browsers – Microsoft Edge, Google Chrome, Mozilla Firefox
Security Software	Locally installed applications and services that detect or prevent the execution of malicious code or enforce organisational security policy on a device. Examples: Kaspersky, Avast, McAfee

These categories represent the most significant risk to the Australian Government's technology estate. This list is not exhaustive and will be expanded, if necessary, as the CTS develops.

Entities are recommended to consider categorising applications and web services in accordance with the above list as part of their application and web service control strategies.

Products, applications and web services may fall into multiple categories. For example, the *Social Media* and *Communications* categories often have significant overlaps. Where overlaps exist, entities should categorise:

- Based on similar applications, products or web services identified on the CTS *Applications Policy* or *Deny List*, or
- apply best judgement based on the examples provided in Table 2.

Where products, applications and web services fall outside of these categories, entities should categorise based on the similar applications and web services included in the examples in Table 2.

2.3. Deny List Additions

A product, application or web service can only be added to the *Deny List* at the decision of the Government Security Committee or the Protective Security Board, derived from a:

- threat report from a Technical Authority Entity
- Technology Vendor Review Framework recommendation, or
- risk product from developed by the Department of Home Affairs.

Additions to the *Deny List* are only made where the addition:

- addresses a significant security risk or opportunity to mitigate risk to the Commonwealth
- provides a proportionate, timely, and flexible mechanism to align the Australian Government with action taken by like-minded nations to address a significant security risk, or
- provides Accountable Authorities of Commonwealth entities with the guidance required to allocate resources to assist the Department of Home Affairs to understand and address a systemic risk.

2.3.1. Implementation and Communication

Additions to the *Deny List* are communicated via email to the Chief Security Officer and generic security email address of all non-corporate Commonwealth entities (NCEs) at OFFICIAL: Sensitive.

Entities will be informed that the updated *Deny List* has been provided to their nominated secret email address if previously provided.

2.3.2. Access to the *Deny List* for Entities Without SECRET Systems

Entities will be instructed to contact their department of state or lead portfolio entity in accordance with the CTS *Deny List* distribution mechanism.

Where necessary, The Department of Home Affairs can facilitate in person viewing. Entities are not expected to retain personnel in business services areas that are security cleared to access SECRET material for the sole purpose of accessing the *Deny List*.

2.3.3. Communications Mechanisms for Additions

Entities will be required to communicate to personnel working in business services areas that products, applications and web services have been added to the *Deny List*, such as Information Technology (IT) and Human Resources (HR) business areas, to facilitate updating of internal blocklist.

The *Deny List* is SECRET in aggregation. Additions can be from OFFICIAL up to SECRET, depending on the mechanism for addition and available threat information.

Where there has been an addition to the *Deny List*, entities will be provided with advice on the security classification in which this update can be communicated.

Entities will be provided with implementation guidance for additions to the *Deny List*, as well as advice on the security classification the additions can be communicated at— including templated language. For example:

> 'The Department of Home Affairs has advised that, in accordance with PSPF Requirement 0221 and the Commonwealth Technology Standard, [product] presents an unacceptable level of security risk to the Australian Government and most not be accessed used or installed on Australian Government systems and mobile devices.'

2.4. Centralised Risk Sharing Capability

PSPF Requirement 0222 mandates that a policy that considers sharing risk assessments of products, applications and web services to the Department of Home Affairs' Centralised Risk Sharing Capability is established.

The Centralised Risk Sharing Capability (CRSC) is a centralised repository for risk assessments of products, applications and web services to eliminate duplicative and inconsistent effort in the risk assessment and decision-making process across the Australian Government for the management of applications in the modern technology environment. It also ensures that foreign ownership, control and influence risks are appropriately and consistently considered.

It is maintained by the Department of Home Affairs and allows the sharing of acceptable risk assessments to reduce burden on entities and the private sector. It will also make the Commonwealth a more efficient procurer of services.

The Centralised Risk Sharing Capability Procedure – Policy Procedure (available on GovTEAMS) has been developed which sets out the Department of Home Affairs and entity processes that operate under the CRSC and the Applications Policy. Sharing risk assessments through the CRSC includes 3 steps:

- submission of security assessments by NCEs to the Department of Home Affairs
- quality assurance evaluation of risk assessments by the Department of Home Affairs, including anonymisation of information, and
- access and distribution of quality-assured risk assessments.

Risk assessment can be provided to the Department of Home Affairs' Commonwealth Security Policy Branch at PSPF@homeaffairs.gov.au.

3. Risk Assessment

PSPF Release 2026 Section 13.4 – Applications Management requires all applications, products, and web services to be approved to be installed or used on resources that access Australian Government technology systems or data. Entities must conduct a risk assessment for any products, applications or web services not listed on either of the CTS *Applications Policy* or *Deny List*.

The *Applications Policy* is **best-practice** and **voluntary**. Entities **must** have an established process when undertaking technology system authorisation that considers applications and web services identified on this list. Entities **may** install applications, products or use web services that appear on this list without conducting a risk assessment. Refer to CTS Section 2 – CTS Applications Policy and Deny List for details.

Refer to PSPF Release 2026 Section 13.3 – Technology System Authorisation for details on the authorisation process for technology systems.

Refer to PSPF Guidelines Section 5.2 – Security Risk Management Process for guidance on conducting security risk assessments.

As part of the risk assessment entities must apply the following PSPF Requirements:

- PSPF Requirement 0039 to ensure procurement and contract decisions do not expose the entity or the Australian Government to an unacceptable level of risk. Refer to PSPF Release 2026 Section 6.1 Procurement, Outsourcing and Contract Management.
- PSPF Requirement 0040 to ensure procurement, contracts and third-party outsourced arrangements, contain proportionate security terms and conditions to ensure service providers, contractors and subcontractors comply with relevant PSPF Requirements and avoid exposing the entity or the Australian Government to an unacceptable level of risk. Refer to PSPF Release 2026 Section 6.1 Procurement, Outsourcing and Contract Management.
- PSPF Requirement 0046 to ensure procurement and contract decisions consider the security risks before engaging providers operating under foreign ownership, control or influence, and in response to any developments during the contract period that may give rise to foreign ownership, control or influence (FOCI) risks. Refer to PSPF Release 2026 Section 6.1.3 Foreign Ownership, Control or Influence in Procurement.
- PSPF Requirement 0049 to manage the security risk associated with engaging foreign partners if the application or web services is not Australian owned and operated. Refer to PSPF Release 2026 Section 7.1 Recognising Foreign Interference and Espionage.
- PSPF Requirement 0062 to protect security classified information. Refer to PSPF Release 2026 Section 9.3 Minimum Protections and Handling Requirements.
- PSPF Requirement 0086 to authorise the application or web services. Refer to PSPF Release 2026 Section 13.3 Technology Systems Authorisation.
- PSPF Requirement 0087 to inform decisions to authorise (or reauthorise) a new technology system or make changes to an existing technology system based on the Information Security Manual's (ISM) risk-based approach to cyber security. Refer to PSPF Release 2026 Section 13.3 Technology Systems Authorisation.

3.1. Foreign Ownership, Control or Influence

PSPF Requirement 0039 requires that the entity is accountable for the management of security risks arising from procuring goods and services and ensures procurement and contract decisions do not expose the entity or the Australian Government to an unacceptable level of risk.

Entities must ensure that all existing requirements under the PSPF, including those pertaining to procurement, third party risk management and countering foreign interference and espionage, are still considered when applying the CTS.

As a result of the unprecedented levels of foreign powers interfering and targeting Australia, Australian Government entities that enter into commercial arrangements with organisations operating under Foreign Ownership, Control or Influence (FOCI) are at increased risk of foreign interference and espionage and must consider this risk as part of their obligations to mitigate security risks.

PSPF Requirement 0046 requires that procurement and contract decisions consider the security risks before engaging providers operating under foreign ownership, control or influence, and in response to any developments during the contract period that may give rise to foreign ownership, control or influence risks.

The Department of Home Affairs has produced guidance on identifying FOCI risks in procurement which includes a template to support contract managers to assess a vendor's exposure to FOCI and correlating security risks.

Refer to the Foreign Ownership, Control, or Influence (FOCI) Risk Assessment Guidance for details.

4. Evaluation and Exemption Process

4.1. Evaluation Process to be added to CTS Applications Policy

The CTS allows entities to request for products, applications and web services be added to the CTS *Applications Policy*. The process involves:

1. Completing the **Evaluation Form** provided at **Annex C**.
2. Submitting the form to the Department of Home Affairs' Commonwealth Security Policy Branch at:
    - PSPF@homeaffairs.gov.au (for requests up to PROTECTED)
    - HomeAffairs_ProtectiveSecurityPolicy@asnet.gov.au (for requests at SECRET)
    - PSPF@homeaffairs.ic.gov.au (for requests at TOP SECRET)
3. The Department of Home Affairs will process the request, conduct a risk assessment and evaluate whether the specified application, product or web service meets the requirements for inclusion on the CTS *Applications Policy* and will notify the requesting entity of the result.

4.2. Exemption Process for a Legitimate Business Reason

The CTS allows the Accountable Authority of an entity to seek an exemption for a legitimate business reason that requires the use of products, applications and web services included on the CTS *Deny List*, provided appropriate mitigations are in place.

The Department of Home Affairs will assess all exemption requests on the grounds of legitimate business reasons, review and agree mitigation strategies and either grant or deny all exemptions. A legitimate business reason must be time limited and follow all mitigations outlined below

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 following mitigation strategies have been approved by ASD in its capacity as the Technical Authority Entity and represent the minimum mitigation strategies that the requesting entity must apply when seeking an exemption:

- Ensure products, applications and web services are only accessed, used or installed on a separate standalone device without access to services that process or access classified information.
- Ensure the separate standalone device is appropriately stored and secured when not in use. This includes the isolation of these devices from security classified conversations and information.
- Minimise, where possible, the input of OFFICIAL or security classified information into products, applications and web services.
- Use an official generic email address (for example, a group mailbox) for any accounts associated with products, applications and web services.
- Ensure that devices that use or access products, applications and web services are using the latest available operating system in order to control individual mobile application permissions. Regularly check for and update applications and products to ensure the latest version is used.
- Only install applications and products from trusted stores such as the Microsoft Store, Google Play Store and the iOS App Store.
- Ensure only authorised users have access to any corporate accounts associated with products, applications and web services, and that access (either direct or delegated) is revoked immediately when there is no longer a requirement for that access.
- Carefully and regularly review the terms and conditions, as well as permissions with each update to products, applications and web services, to ensure appropriate risk management controls can be put in place or adjusted as required.
- Delete applications and products from devices when access is no longer required.
- Implement strategies to identify and log unauthorised installation or use of products, applications and web services on systems and devices, and to audit those logs for oversight purposes.

Entities must also implement relevant PSPF Requirements and ISM controls.

4.2.1. Exemption Process

The process for requesting an exemption and the ongoing management of authorised use of applications listed on the CTS *Deny List* involves:

1. Completing the Exemption Form provided at Annex D.
    - The form requires entities to specify which application or web services the entity is seeking an exemption to use,

- provide the legitimate reason along with details about the functions that necessitate the exemption, indicate the time period the exemption is required for, and
- identify the mitigations the entity will employ to minimise the security risks associated with use.

2. Submitting the form to the Department of Home Affairs' Commonwealth Security Policy Branch at:
   - PSPF@homeaffairs.gov.au (for requests up to PROTECTED)
   - HomeAffairs_ProtectiveSecurityPolicy@asnet.gov.au (for requests at SECRET)
   - PSPF@homeaffairs.ic.gov.au (for requests at TOP SECRET)
3. The Department of Home Affairs will consider the request from a whole-of-government risk perspective and review the proposed mitigation strategies against the minimum strategies prescribed by ASD.
   - The requesting entity may be contacted if further information regarding proposed mitigation strategies is required.
   - The Department of Home Affairs will advise the requesting entity of the outcome.
4. Where an exemption is granted, the entity's Accountable Authority must:
   - acknowledge and accept residual risks,
   - document arrangements of the exemption and acceptance of residual risks in the entity's security plan,
   - ensure compliance with all other relevant PSPF requirements on security risk management, and
   - report on exemption arrangements in the annual PSPF reporting process.

5. Glossary

5.1. Glossary of Abbreviations

Term	Definition
ASD	Australia Signals Directorate
CTS	Commonwealth Technology Standard
FOCI	Foreign ownership, control or influence
ISM	Information Security Manual
NCE	Non-corporate Commonwealth entity
PSPF	Protective Security Policy Framework

5.2. Glossary of Terms

Term	Definition
Applications Policy	The list of products, applications and web services that entities **may** use or access, without needing to conduct a risk assessment.
Accountable Authority	The person or people responsible for, and with control over, a Commonwealth entity's operations. This is set out in Section 12 of the Public Governance, Performance and Accountability Act 2013 (Cth).
Communications	Constitutes applications and services that are facilitate direct messaging or sharing of information between individual recipients or small groups of recipients.
Deny List	The list of products, applications and web services that entities **must not** install or access, except in the case of a legitimate business reason.
Entity	Any Commonwealth entity listed under paragraph 10(1) of the PGPA Act. For the purposes of the PSPF Requirements and the Australian Government Commonwealth Technology Standard (CTS), entity refers to non-corporate Commonwealth entities (NCEs).
Extrajudicial Direction	A direction issued by an actor outside of, or without the permission of, the official legal system or legislation within the relevant jurisdiction.
Gateway	Gateways securely manage data flows between connected networks from different security domains.
Hardware	A generic term for IT equipment and OT equipment
Information	Physical documents/papers, electronic/digital data or intellectual information (knowledge) that is owned, managed or maintained by the entity. It includes details of methodologies, classified military/intelligence activities or operations, diplomatic discussions and negotiations.
Mobile Device	A portable computing or communications device, including smart phones, handheld computers, tablets, laptops and digital assistants that use a mobile operating system.
Mobile Device (Government-Issued)	Mobile or portable computing communications device that is owned and issued by an Australia Government entity to access government systems and information, configured, encrypted and managed to ASD standards and guidance and is approved by the relevant authority to process, store or communicate entity information of a specified classification. This includes Australian Government-issued mobile devices

Term	Definition
	that for operational reasons are connected to isolated networks, for example standalone or air gapped devices.
Mobile Device (Authorised Non-Government)	Mobile or portable computing communications devices owned or issued by a non-government source (for example commercial organisation, non-government organisation, industry-issued or privately owned) that is configured, encrypted and managed in accordance with ASD standards and guidance, and the residual risk is accepted by the Australian Government entity system risk owner to access, process, store or communicate OFFICIAL, OFFICIAL: Sensitive, PROTECTED Australian Government information or data.
Mobile Device (Other Non-Government)	Devices that are not owned, issued or authorised by the entity. Includes radio frequency and infrared devices such as private mobile phones, devices, wireless keyboards, Bluetooth devices, smart watches, cameras and any other infrared device that is capable of recording or transmitting audio or data. These devices must not be authorised to access, process, store or communicate government OFFICIAL: Sensitive or above information, and must not enter Zones 4-5 or where SECRET or TOP SECRET information or devices are present.
Office Productivity Tools	Constitutes applications and services that are intended to be used to produce, format and adjust the display of information produced as part of day to day office work. Examples include word processors, spreadsheet applications, PDF readers, and web browsers.
Security Software	Constitutes locally installed applications and services that detect or prevent the execution of malicious code or enforce organisational security policy on a device.
Social Media	Constitutes applications and services that are intended to facilitate the creation, sharing and aggregation of content for consumption by the public or large communities.
System	Related set of hardware, software and supporting infrastructure used for the processing, storage or communication of information/data and the governance framework in which it operates.
System Owner	Person responsible for ensuring the secure operation of the technology system.
Technical Manual	Technical Manuals are standard or technical controls authorised by the PSPF and maintained by the relevant Technical Authority Entity.
Technology System	Collective term for information technology and operational technology systems.

ANNEX A – Commonwealth Technology Standard Applications Policy

The Australian Government Commonwealth Technology Standard *Application Policy* represents applications and web services that have been assessed as being acceptable for use by Australian Government entities. It acts as an enabler for Commonwealth entities, is **best-practice** and **voluntary**. The *Applications Policy* is not exhaustive and is best-practice guidance based on the Centralised Risk Sharing Capability operated by the Department of Home Affairs.

Due to its content, **ANNEX A** is security classified at SECRET.

To request a copy, contact the Department of Home Affairs' Commonwealth Security Policy Branch at PSPF@homeaffairs.gov.au with an appropriate email address capable of receiving SECRET information.

Entities that do not operate technology systems authorised to the SECRET level may request for a physical, hard-copy version of the *Applications Policy*.

ANNEX B – Commonwealth Technology Standard Deny List

The Australian Government Commonwealth Technology Standard (CTS) *Deny List* represents products, applications and web services that have been assessed as presenting an unacceptable risk to the Australian Government's technology estate. The CTS Deny List provides Australian Government entities with a security classified, repeatable, low-risk process for managing increasingly complex application risk. Implementation of the *Deny List* is **mandatory** for all non-corporate Commonwealth Entities (NCEs).

Due to its content, **ANNEX B** is security classified at **SECRET**.

To request a copy, contact the Department of Home Affairs' Commonwealth Security Policy Branch at PSPF@homeaffairs.gov.au with an appropriate email address capable of receiving SECRET information.

Entities that do not operate technology systems authorised to the SECRET level may request for a physical, hard-copy version of the *Deny List.*

ANNEX C – Applications Policy Evaluation Request Form

The Australian Government Commonwealth Technology Standard (CTS) allows entities to request that products, applications and web services be added to the CTS *Applications Policy*. This permits entities to install, access or use these without having to conduct a risk assessment as part of the technology authorisation process.

The Department of Home Affairs will process the request and evaluate whether the specified application or web services meets the requirements for inclusion on the CTS *Applications Policy*.

Commonwealth Technology Standard – Applications Policy Evaluation Request Form		
Entity Name	[Australian Government entity name]	
Accountable Authority	[Name of the entity's Accountable Authority]	
Entity Contact Officer	Name:	Position:
	Email:	Phone:
Application, Product or Web Service Name		
Application, Product or Web Service Category	[Specify the category of application, product or web service the entity is seeking an evaluation. Refer to Table 1 for the CTS categories]	
Vendor	[Vendor of the application, product or web service]	
Model Number	[Model number of the application, product or web service if applicable]	
Software Version	[Software version of the application, product or web service]	
Notes	[Optional space for entity to provide any additional information to support the request]	

Submit completed form to Department of Home Affairs at: PSPF@homeaffairs.gov.au (up to PROTECTED); HomeAffairs_ProtectiveSecurityPolicy@asnet.gov.au (SECRET); PSPF@homeaffairs.ic.gov.au (TOP SECRET).

INTERNAL USE – DEPARTMENT OF HOME AFFAIRS

Evaluation Decision	Approved: ☐	Not Approved: ☐
Dates	Date Approved:	
Evaluation Approval	Name:	Position:
	Email:	Phone:
Record	[Content Manager reference]	

ANNEX D – Deny List Exemption Request Form

The Australian Government Commonwealth Technology Standard (CTS) provides that the Accountable Authority may seek an exemption to use products, applications and web services for a legitimate business reason.

The Department of Home Affairs will assess all exemption requests on the grounds of legitimate business reasons, review and agree mitigation strategies, and either grant or deny all exemptions. A legitimate business reason includes:

- 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.

***Deny List* Exemption Request Form**		
Entity Name	[Australian Government entity name]	
Accountable Authority	[Name of the entity's Accountable Authority]	
Contact Officer	Name:	Position:
	Email:	Phone:
Legitimate Reason	National Security function: ☐	Regulatory function: ☐
Application, Product and Web Service Category	[Specify the category of which application, product or web service the entity is seeking an exemption to use]	
Time Period	[Specify how long the exemption is required for]	
Mitigation Strategies	• [List proposed mitigation strategies to minimise associated security risks]	
Notes	[Optional space for entity to provide any additional information to support the request]	

Submit completed form to Department of Home Affairs at: PSPF@homeaffairs.gov.au (up to PROTECTED); HomeAffairs_ProtectiveSecurityPolicy@asnet.gov.au (SECRET); PSPF@homeaffairs.ic.gov.au (TOP SECRET).

INTERNAL USE – DEPARTMENT OF HOME AFFAIRS

Exemption Decision	Approved: ☐	Not Approved: ☐
Dates	Date Approved:	Date Exemption Expires:
Exemption Approval	[Approving officer's Name, Position, Email]	
ASD Prescribed Mitigation Strategies	• [List prescribed mitigation strategies]	
Record	[Content Manager reference]	