9 Access to information

A. Purpose

1. This policy details security protections that support entities' provision of timely, reliable and appropriate access to official information. Providing access to information helps develop new products and services, can enhance consumer and business outcomes and assists with decision-making and policy development.
2. Access to government information does not need to be limited for security purposes, except in select circumstances as identified in the requirements (primarily when sharing sensitive or classified information, or disclosing information outside government).

B.Requirements

B.1 Core requirement

Each entity must enable appropriate access to official information. This includes:

- ***a. sharing information within the entity, as well as with other relevant stakeholders***
- ***b. ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information, and***
- ***c. controlling access (including remote access)to supporting ICT systems, networks, infrastructure, devices and applications.***

B.2 Supporting requirements

Supporting requirements for access to information

<table>
<tr><th>#</th><th>Supporting requirements</th></tr>
<tr><td>Requirement 1.
Formalised agreements for sharing information and resources</td><td>When disclosing security classified information or resources to a person or organisation outside of government, entities must have in place an agreement or arrangement, such as a contract or deed, governing how the information is used and protected.</td></tr>
<tr><td>Requirement 2.
Limiting access to sensitive and classified information and resources</td><td>To reduce the risk of unauthorised disclosure, entities must ensure access to sensitive and security classified information or resources is only provided to people with a need-to-know.</td></tr>
<tr><td>Requirement 3.
Ongoing access security classified information and resources</td><td>a. Entities must ensure that people requiring ongoing access to security classified information or resources are security cleared to the appropriate level:
<table><tr><td></td><td colspan="3">Security classified information</td></tr><tr><td></td><td>PROTECTED</td><td>SECRET</td><td>TOP SECRET</td></tr><tr><td>Personnel security clearance for ongoing access</td><td>Baseline security clearance or above.</td><td>Negative Vetting 1 security clearance or above.</td><td>Negative Vetting 2 security clearance or above.</td></tr></table>Note I Some Australian office holders are not required to hold a security clearance.
b. In addition, entities must ensure that people requiring access to caveated information meet all clearance and suitability requirements imposed by the originator and caveat owner.</td></tr>
<tr><td>Requirement 4.
Temporary access to</td><td>Entities may provide a person with temporary access to security classified information or resources on the basis of a risk assessment for each case. In such cases, entities must:</td></tr>
</table>

#	Supporting requirements
classified information and resources	a. limit the duration of access to security classified information or resources: i. to the period in which an application for a security clearance is being processed for the particular person, or ii. up to a maximum of three months in a 12-month period b. conduct recommended employment screening checks (see the PSPF policy: Eligibility and suitability of personnel) c. supervise all temporary access d. for access to TOP SECRET information, ensure the person has an existing Negative Vetting 1 security clearance, and e. deny temporary access to caveated information (other than in exceptional circumstances, and only with approval of the caveat owner).
Requirement 5 Managing access to information systems	To manage access to information systems holding sensitive or security classified information, entities **must** implement unique user identification, authentication and authorisation practices on each occasion where system access is granted.

C.Guidance

C.1 Sharing information in the entity and with external stakeholders

3. **Requirement 1** mandates that written agreements, such as contracts or deeds, are in place to protect classified information disclosed to non-government stakeholders. This includes external parties accessing, processing, communicating or managing information assets, or adding products, services or functions to government information systems.
4. Risks may arise when information is shared outside of government. This is because PSPF information handling and protection requirements apply only to government unless included in an agreement, such as a contract or deed. Even where these instruments exist, there may be limited avenues for recourse in the event of a security incident.
5. Agreements for information disclosure provide assurance that external stakeholders understand the obligations to protect government information. The Attorney-General's Department recommends that entities consider using written agreements to protect all government information disclosed externally especially where that information is sensitive.
6. The following factors may be relevant to considering whether to require a written agreement before sharing information:
    a. if the information is subject to s95B of the Privacy Act that mandates entities take contractual measures to ensure that a contracted service provider does not do an act, or engage in a practice, that would breach an Australian Privacy Principle.
    b. if the information is subject to any legislative secrecy provisions
    c. whether the aggregation of information to be shared increases the business impact level of potential compromise
    d. what type of access is being granted and the level of supervision and control that the entity will have over the personnel granted access.
7. The Attorney-General's Department recommends entities put in place regular monitoring of the security controls, service definitions and delivery levels that are included in deeds or contract agreements to assist the implementation of PSPF protections. This can include regular reviews and audits of services, reports and records. For guidance, see the PSPF policy: Security governance for contracted goods and service providers.
8. The PSPF policy: Security governance for international sharing requires an agreement or arrangement to be in place for a foreign national to access classified information.

Legislative provisions on access to information

Commonwealth legislation, common law and policy regulate the disclosure of sensitive information. This includes relevant secrecy provisions, privacy law and legal professional privilege that restrict information access in some cases.[1]

It may be an offence under the *Crimes Act 1914* or Criminal Code to share or disclose information inappropriately. In addition, under some legislation, it may be necessary to limit sharing of information depending on the purpose for which it was collected. Some government policy and legislation may also require agreement or consent to disclose information (eg sharing sensitive personal information covered by Australian Privacy Principles[2]).

C.2 Limiting access to sensitive and classified information to those who need to know

9. The need-to-know principle applies to all sensitive and classified information. It reflects the need for personnel to access this information only where there is an operational requirement to do so. The practice helps personnel understand their responsibility to protect information, including the correct methods for storage, handling and dissemination.

10. **Requirement 2** mandates that access to, and dissemination of, sensitive and security classified information is limited to personnel who need the resources to do their work. This involves:

    a. providing access to information only to personnel who need that access; not based on convenience or because of their status, position, rank or level of authorised access

    b. a positive obligation to share relevant information so that people with an operational need-to-know the information have access.

C.3 Personnel security clearances for access to classified information

11. Access to sensitive and security classified information necessitates a high level of assurance of a person's integrity. This is due to the potential harm associated with compromise of that information.

12. In addition to having a need-to-know (as per **Requirement 2**), **Requirement 3** limits access to security classified information to those with the necessary security clearance.

13. Minimum security clearance levels for access to each information classification level are detailed in Table 1.

Table 1 Minimum security clearance levels for ongoing access to information

		Sensitive information	Security classified information		
	OFFICIAL		PROTECTED	SECRET	TOP SECRET
		OFFICIAL: Sensitive			
Personnel security clearance for ongoing access	Security clearance not required (For entity personnel, employment screening is sufficient).	Security clearance not required (For entity personnel, employment screening is sufficient).	Baseline security clearance or above.	Negative Vetting 1 security clearance or above.	Negative Vetting 2 security clearance or above.

14. Access to caveated information that involves a codeword requires a briefing and may require a Negative Vetting 1, Negative Vetting 2 level or Positive Vetting level security clearance as well as other additional requirements. See C.3.2 Access to caveated information below.

15. For information regarding personnel security clearance assessments, see the PSPF policy: Eligibility and suitability of personnel.

C.3.1 Australian office holders who do not need a security clearance

16. Some Australian office holders are not required to hold a security clearance to access security classified information while exercising the duties of the office (however, staff of these office holders are not exempt from security clearance requirements). Australian office holders who do not need a security clearance are:

[1] In 2010, Australian Law Reform Commission Report 112: Secrecy Laws and Open Government in Australia identified 506 secrecy provisions in 176 pieces of legislation, including 358 distinct criminal offences.
[2] See the OAIC Guide to securing personal information for entities covered by the Privacy Act regarding access controls to protect personal information.

a. members and senators of the Commonwealth and state parliaments and territory legislative assemblies
b. judges of federal courts and the Supreme Courts of the states and territories
c. royal commissioners
d. the Governor-General, state governors, the Northern Territory administrator
e. members of the Executive Council, and
f. appointed office holders with enabling legislation that gives the same privileges as the office holders already identified eg members of the Administrative Appeals Tribunal.

C.3.2 Access to caveated information

17. Stringent protections apply to caveated information. **Requirement 3** mandates that people requiring access to caveated information meet all clearance and suitability requirements imposed by the originator and caveat owner. These requirements are established in PSPF policy: Sensitive and classified information and the supporting Security Caveats Guidelines (available to security advisors only on GovTEAMS or by request).
18. Of particular note, the three releasability caveats—Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) and Releasable to (REL)—limit access to information based on citizenship.
    a. Entities **must not** share information bearing the AUSTEO caveat with a person **who is not** an Australian citizen (dual citizenship does not preclude access).
        i. If there is a business need to share AUSTEO information with a person who is not an Australian citizen, the originator can, on a case-by-case basis, reconsider application of the AUSTEO caveat to its information and, if warranted, apply a different caveat or classification to that information (eg the AGAO or REL caveat). For guidance on reclassifying information, see the PSPF policy: Sensitive and classified information.
    b. Entities, other than the Australian Signals Directorate, Australian Security Intelligence Organisation, Australian Secret Intelligence Service, the Department of Defence and Office of National Intelligence, **must not** share information bearing the AGAO caveat with a person who is not an Australian citizen.
        i. AGAO material is releasable to appropriately cleared representatives of Five-Eyes foreign governments on exchange or long-term posting or attachment in the Australian Signals Directorate, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Department of Defence or the Office of National Intelligence.
19. Supporting requirements in the PSPF policy: Security governance for international sharing limit foreign access to sensitive and security classified information that is subject to a releasability caveat even when an international agreement or arrangement is in place that would otherwise permit sharing classified information.

C.4 Temporary access to classified resources

20. Temporary (rather than ongoing access) to classified information may be required in some limited circumstances. Temporary access may be provided up to and including SECRET level information without a security clearance, after the risks of doing so have been assessed. Temporary access to TOP SECRET information requires an existing Negative Vetting 1 security clearance.
21. Temporary access to security classified information includes:
    a. short-term access, where the person does not hold a clearance at the appropriate level (but has a valid need-to-know and requires access to relevant information) and the risks can be mitigated. This may include, but is not limited to:
        i. new starters
        i. people on short-term projects

ii. people who are reasonably expected to have only incidental or accidental contact with security classified information (eg security guards, cleaners, external IT personnel, researchers and visitors such as children who do not have an ability to comprehend the classified information[3])

b. provisional access, where the person has commenced a clearance process by providing the relevant details for assessment by a vetting agency.

22. The type of temporary access can be changed from short-term to provisional once the vetting agency has confirmed that the completed security clearance pack has been received and advises the entity that no initial concerns have been identified.

23. **Requirement 4** mandates the following minimum protections to safeguard classified resources that are accessed on a temporary basis:

a. entities must limit the duration of access to security classified information as follows:

i. for short-term access – a maximum of three months in a 12-month period

ii. for provisional access – until a security clearance is granted or denied

b. entities must supervise all temporary access. Examples include:

i. escorting visitors in premises where classified information is being stored or used

ii. management oversight of the work of personnel who have the temporary access

iii. monitoring or audit logging incidents of contact with security classified information[4] (eg contract conditions that require service providers to report when any of their contractors have had contact with classified information).

c. entities must ensure that personnel have an existing Negative Vetting 1 security clearance for short-term or provisional access to TOP SECRET information.

d. in exceptional circumstances, short-term or provisional access to caveated information may be granted by the originator and caveat owner based on assessed risk and granted on a case-by-case basis. For further information see section C.3.2.

24. **Requirement 4** mandates that entities conduct a risk assessment to determine whether to allow temporary access to classified information. The Attorney-General's Department recommends the assessment include:

a. the need for temporary access, including if the role can be performed by a person who already holds the necessary clearance

b. confirmation from the authorised vetting agency that the person has no identified security concerns, or a clearance that has been cancelled or denied

c. the quantum and classification level of information that could be accessed, and the potential business impact if this information was compromised

d. how access to classified information will be supervised, including how access to caveat or compartmented information will be prevented, and

e. other risk mitigating factors such as pre-engagement screening, entity specific character checks, knowledge of personal history, or having an existing or previous security clearance.

25. Where an entity intends to grant temporary access to classified information from another entity or third party, the Attorney-General's Department recommends consulting the other entity or party, where appropriate, and obtaining agreement for temporary access to their classified information.

26. The Attorney-General's Department considers there is merit in obtaining an undertaking (eg through a confidentiality or non-disclosure agreement) from the person to protect official information.

[3] The Attorney-General's Department considers this to be children aged under 10 years.

[4] Monitoring and audit logging (and related audit trails) are key measures to control access to ICT systems and the information held on those systems. Further information about developing and maintaining robust ICT systems is included under the PSPF policy: Robust ICT systems.

C.5 Information access controls

27. Having well structured, robust ICT systems provides access for personnel to undertake their work. It also protects information, technology and intellectual property.

28. Access to networks, operating systems, applications and sensitive or classified information that is processed, stored or communicated is controlled through:

    a. a clear understanding of the information held on such systems, and

    b. effective user identification and authentication practices.

29. For guidance on ICT system development, see the PSPF policy: Robust ICT systems.

C.5.1 User identification, authentication and authorisation practices

C.5.1.1 User identification and authentication

30. Entities are encouraged to establish a formal user registration and de-registration procedure for granting and revoking access; this helps entities have confidence about who is accessing their information. The Attorney-General's Department recommends entities regularly review user access rights; this provides confidence that users can only access the sensitive or security classified information they have been specifically authorised to use.

31. Having uniquely identifiable users helps to ensure accountability. Authenticating the identity of users on each occasion that system access is granted helps provide assurance that information is being accessed appropriately. Entities can authenticate access by various methods including:

    a. passphrases or passwords

    b. biometrics

    c. cryptographic tokens

    d. smart cards.

32. Entities may reduce the risk of user accounts being compromised by:

    a. using multi-factor authentication (two or more authentication methods) where users provide something they know, like a passphrase; something they have, like a physical token; and/or something they are, like biometric data

    b. increasing the complexity of single authentication methods (such as passphrases or passwords) by increasing the minimum password length and using a mix of alphanumeric and special characters.

33. Systems and network managers normally need increased administrative access rights to perform their jobs. This implies a high degree of trust and stringent controls to balance the need for privileged access to systems and networks against risks to these peoples' trustworthiness and competence.

34. The Attorney-General's Department recommends using multi-factor authentication to assure the identity of a higher-risk user. This includes system administrators, database administrators, privileged users (and other similar positions of trust) as well as remote access users. Strengthened personnel and physical security controls for privileged access can also be beneficial.

35. For guidance, see the PSPF policy: Safeguarding information from cyber threats (in particular, the supporting requirement, Restricting administrative privileges). Technical guidance is available in the Australian Government Information Security Manual.

C.5.1.2 Authorising access to ICT systems

36. Sound authorisation measures allow entities to effectively control access to their information, ICT systems, networks (including remote access), infrastructure and applications. The Attorney-General's Department recommends that entities implement measures to manage authorised access to systems holding its sensitive and classified information as detailed in **Table 2**. Further information and technical guidance is available in the Australian Government Information Security Manual.

Table 2 Recommended access authorisation measures

Type of access	Recommended measures
User access management	Ensure that systems for managing passwords are interactive and require users to follow good security practices in the selection and use of passwords or passphrases.
Authorised network access	Consider the use of automatic equipment identification as a means to authenticate connections from specific locations and equipment. Control physical and logical access to diagnostic and configuration ports. Restrict the ability of users to connect to shared networks, including those that extend across entity boundaries. Segregate groups of information services, users and information systems, based on an entity risk assessment. Implement routing controls for networks to ensure computer connections and information flows do not breach other relevant access management measures.
Authorised operating system access	Control access to operating systems through a secure log-on procedure. Restrict and tightly control the use of utility programs that may be capable of overriding system and application controls. Display restricted access and authorised use only (or equivalent) warnings upon access to all entity ICT systems, and shut down inactive sessions after a defined period of inactivity. Consider restricting connection times to provide additional security for high risk applications.
Application and information access	Afford sensitive systems a dedicated (isolated) computing environment, in accordance with entity risk assessment.
Mobile computing and communications	Adopt security measures to protect against the risks of using mobile computing and communications facilities.

D. Find out more

37. Other legislation and policies:
    a. Australian Signals Directorate Information Security Manual
    b. Office of the Australian Information Commissioner Guide to securing personal information for Australian Government entities covered by the *Privacy Act 1988*
    c. ACSI 53 – Communications Security Handbook (Rules and Procedures for Agency Comsec Officer and Custodian). Available to Comsec officers via ASD.
38. Further guidance and support is available in the Australian Standard AS/NZS ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management.

D.1 Change log

Table 3 Amendments in this policy

Version	Date	Section	Amendment
V2018.1	Sep 2018	Whole document	This is the first issue of this policy
V2018.2	Nov 2018	C.3.1	Reference to dual citizenship
V2018.3	Oct 2019	Core requirement	Amendment to capture devices and ensure consideration of remote access apply to all of part c
		Supporting requirements	Removing requirement for written agreement for sensitive information
			Clarifying that security clearance requirements only apply to classified information
		C.1	Amended guidance to reflect changes to requirement 1
		C.3.2	Clarify application of caveats and access restrictions in the Australian Government Security Caveats Guidelines
		C.5	Content moved to PSPF Policy 8: Sensitive and classified information