8 Sensitive and security classified information

A. Purpose

1. This policy details how entities correctly assess the sensitivity or security classification of their information and adopt marking, handling, storage and disposal arrangements that guard against information compromise.
2. Information is a valuable resource. Protecting the confidentiality, integrity and availability of information is critical to business operations.
   a. **Confidentiality** of information refers to the limiting of access to information to authorised persons for approved purposes.
   b. **Integrity** of information refers to the assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid.
   c. **Availability** of information refers to allowing authorised persons to access information for authorised purposes at the time they need to do so.
3. A security classification (PROTECTED, SECRET and TOP SECRET) is only applied to information (or assets that hold information, such as laptops, USBs) if it requires protection because the impact of compromise of the information or asset would be high or above.
4. The requirements in this policy do not displace obligations imposed on entities through other policies, legislation or regulations, or by any other means.

B. Requirements

B.1 Core requirement

Each entity must:

a. identify information holdings

b. assess the sensitivity and security classification of information holdings, and

c. implement operational controls for these information holdings proportional to their value, importance and sensitivity.

B.2 Supporting requirements

Supporting requirements help Australian Government entities maintain the confidentiality, integrity and availability of official information—including where the entity is the originator of information (the entity that initially generated or received the information).

Supporting requirements

#	Supporting requirements
Requirement 1. Identifying information holdings	The originator **must** determine whether information being generated is official information (intended for use as an official record) and whether that information is sensitive or security classified.

Requirement 2. Assessing sensitive and security classified information

a. To decide which security classification to apply, the originator **must**:
   i. assess the value, importance or sensitivity of official information by considering the potential damage to government, the national interest, organisations or individuals, that would arise if the information's confidentiality was compromised (refer to the following table), and
   ii. set the security classification at the lowest reasonable level.

b. The originator must assess the information as OFFICIAL: Sensitive if:
   i. a security classification does not apply, and
   ii. compromise of the information's confidentiality may result in limited damage to an individual, organisation or government generally.

			Sensitive information	Security classified information		
	UNOFFICIAL	**OFFICIAL**	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
	No business impact	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Compromise of information confidentiality would be expected to cause ➔	**No damage**. This information does not form part of official duty.	**No or insignificant damage.** This is the majority of routine information.	**Limited damage** to an individual, organisation or government generally if compromised.	**Damage** to the national interest, organisations or individuals.	**Serious damage** to the national interest, organisations or individuals.	**Exceptionally grave damage** to the national interest, organisations or individuals.

Requirement 3. Declassification

The originator **must** remain responsible for controlling the sanitisation, reclassification or declassification of the information. An entity **must not** remove or change information's classification without the originator's approval.

Requirement 4. Marking information

The originator **must** clearly identify sensitive and security classified information, including emails, using applicable protective markings by:

a. using text-based protective markings to mark sensitive and security classified information (and associated metadata), unless impractical for operational reasons
b. if text-based protective markings cannot be used, using colour-based protective markings, or
c. if text or colour-based protective markings cannot be used (eg verbal information), applying the entity's marking scheme for such scenarios. Entities **must** document a marking scheme for this purpose and train personnel appropriately.

Requirement 5. Using metadata to mark information

Entities **must** apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process or communicate sensitive or security classified information:

a. for security classified information, apply the 'Security Classification' property (and where relevant, the 'Security Caveat' property)
b. for OFFICIAL: Sensitive information, apply the 'Dissemination Limiting Marker' property
c. where an entity wishes to categorise information content by the type of restrictions on access, apply the 'Rights' property.

Requirement 6. Caveats and accountable material

a. Caveats **must** be marked as text and only appear in conjunction with a security classification.
b. Entities **must** ensure that accountable material:
   i. has page and reference numbering
   ii. is handled in accordance with any special handling requirements imposed by the originator and caveat owner, and
   iii. has an auditable record of all incoming and outgoing material, transfer, copy or movements.
c. For all caveated information, entities **must** apply the protections and handling requirements established by caveat owners in the Australian Government Security Caveats Guidelines.

Requirement 7. Storage

Entities **must** ensure sensitive and security classified information is stored securely in an appropriate security container for the approved zone in accordance with the minimum protection requirements set out in **Annexes A to D**.

Requirement 8. Transfer

Entities **must** ensure sensitive and security classified information is transferred and transmitted by means that deter and detect compromise and that meet the minimum protection requirements set out in **Annexes A to D**.

Requirement 9. Disposal

Entities **must** ensure sensitive and security classified information is disposed of securely in accordance with the minimum protection requirements set out in **Annexes A to D**. This includes ensuring sensitive and classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.

C. Guidance

C.1 Official information

5. Official information is all information created, sent or received as part of the work of the Australian Government. This information is an official record and it provides evidence of what an entity has done and why.
6. Official information can be collected, used, stored and transmitted in many forms including electronic, physical and verbal (eg conversations and presentations).
7. The National Archives of Australia Australian Government Information Management Standard notes that information is a valuable asset. It contributes to good government through supporting efficient business, informing decision-making, demonstrating government accountability and transparency, mitigating risks, adding economic value and protecting rights and entitlements.
8. It is a core requirement of this policy that entities implement operational controls to protect information holdings in proportion to their value, importance and sensitivity. Although this policy is focused on sensitive and security classified information, all official information requires an appropriate degree of protection as information (and assets holding information) are subject to both intentional and accidental threats. In addition, related processes, systems, networks and people have inherent vulnerabilities. A deliberate or accidental threat that compromises information security could have an adverse impact on government business.
9. The Attorney-General's Department recommends entities apply the minimum protections outlined in **Annex E** for OFFICIAL information that is not assessed as being sensitive or security classified information.
10. Information compromise includes, but is not limited to:
    a. loss
    b. misuse
    c. interference
    d. unauthorised access
    e. unauthorised modification
    f. unauthorised disclosure.

C.2 Sensitive and security classified information

11. **Requirement 1** mandates that the originator (the entity that initially generated the information, or received the information from outside the Australian Government) determine whether official information is sensitive or security classified information.
12. The Australian Government uses three security classifications: PROTECTED, SECRET and TOP SECRET. The relevant security classification is based on the likely damage resulting from compromise of the information's confidentiality.
13. Where compromise of the information's confidentiality would cause limited damage but does not warrant a security classification, that information is considered sensitive and is treated as OFFICIAL: Sensitive.
14. All other information from business operations and services requires a routine level of protection and is treated as OFFICIAL. Information that does not form part of official duty is treated as UNOFFICIAL.
15. OFFICIAL: Sensitive, OFFICIAL and UNOFFICIAL are not security classifications.
16. The below guidance also relates to assessing whether an asset (eg a laptop) holds security classified information, and as such is treated as a classified asset. Assets containing sensitive information may also need protection.

C.2.1 Proper use of security classifications

17. It is important that the management of information enables agencies to meet business, government and community needs and expectations—this involves balancing the need to protect information with the need to ensure appropriate access. Appropriately limiting the quantity, scope or timeframe of sensitive and security classified information:
    a. promotes an open and transparent democratic government
    b. provides for accountability in government policies and practices that may be subject to inappropriate or over-classification
    c. allows external oversight of government operations and programs
    d. promotes efficiency and economy in managing information across government.
18. Over-classification of information can result in:
    a. access to official information being unnecessarily limited or delayed
    b. onerous administration and procedural overheads that add to costs
    c. classifications being devalued or ignored by personnel and receiving parties.
19. It is not consistent with this policy to apply a security classification to information in order to:
    a. restrain competition
    b. hide violations of law, inefficiency, or administrative error to prevent embarrassment to an individual, organisation or entity
    c. prevent or delay the release of information that does not need protection.

C.2.2 Who assesses information sensitivity or security classification

20. The person responsible for generating or preparing information on behalf of an entity (or for actioning information produced outside the Australian Government) assesses whether the information is sensitive or needs to be security classified.
21. Only the originator can change the sensitivity or security classification applied to its information. If the application of a classification is considered inappropriate, the original classification decision can be queried with the originator.

C.2.3 When to assess information sensitivity or security classification

22. Assessing the sensitivity or security classification of information when it is first created, or received from outside the Australian Government, helps protect the information. The originator can also set a specific date or event for automatic declassification (for guidance on declassification, refer to C.2.5 Sanitising, reclassifying or declassifying information).

C.2.4 How to assess information sensitivity or security classification

23. **Requirement 2** mandates that the originator assess the sensitivity or security classification of information by considering the potential impact on the national interest, government, organisations or individuals that could arise from compromise of the information's confidentiality.
24. The more valuable, important or sensitive the official information, the greater the impact on government business that would result from its compromise. By assessing the 'Business Impact Level' if confidentiality of the information is compromised, the originator can determine whether information requires a security classification, is sensitive or requires a routine level of protection.
25. The Business Impact Levels tool (see **Table 1**) provides examples of potential damage from compromise of information's confidentiality. The tool assists in the consistent classification of information and the assessment of impacts on government business.

26. The potential damage from compromise of information's confidentiality determines the classification of that information. A simple flow diagram is provided at **Figure 1** to help assess whether information is sensitive or security classified, based on the potential damage from compromise of the information's confidentiality.

27. The Business Impact Levels tool can also be used for secondary assessments of the potential damage from compromise of the availability or integrity of information. While assessing the Business Impact Level of compromise of the information's availability or integrity does not affect whether the information is sensitive or security classified information, it may indicate that additional security measures (such as ICT, personnel or physical controls) could be warranted.

28. Guidance on minimum protections for handling information that is assessed and determined to be sensitive or security classified is provided at C.5 Minimum protections for sensitive and security classified information.

Examples of OFFICIAL: Sensitive information

Examples of OFFICIAL: Sensitive information may include:

- official information governed by legislation that restricts or prohibits its disclosure, imposes certain use and handling requirements, or restricts dissemination (such as information subject to legal professional privilege or some types of 'personal information', including 'sensitive information' under section 6 of the *Privacy Act 1988* that may cause limited harm to an individual if disclosed or compromised). Where compromise of personal information, including sensitive information (under the Privacy Act) would lead to damage, serious damage or exceptionally grave damage, this information warrants classification. Financial details and tax file numbers may be another example of OFFICIAL: Sensitive information—while they are not sensitive information for the purposes of the Privacy Act, the compromise of this information could still lead to limited damage to individuals.
- commercial or economic data that, if compromised, would undermine an Australian organisation or company, or
- official information that, if compromised, would impede development of government policies.

Table 1 Business Impact Levels tool – Assessing damage to the national interest, government, organisations or individuals

		Sensitive information	Security classified information		
	OFFICIAL		**PROTECTED**	**SECRET**	**TOP SECRET**
		OFFICIAL: Sensitive			
	1 Low business impact	**2 Low to medium business impact**	**3 High business impact**	**4 Extreme business impact**	**5 Catastrophic business impact**
Sub-impact category ⬇	**The majority of official information created or processed by the public sector.** This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in **no or insignificant damage to individuals, organisations or government.**	**OFFICIAL information that due to its sensitive nature requires limited dissemination.** OFFICIAL: Sensitive is not a security classification. It is a dissemination limiting marker (DLM), indicating compromise of the information would result in **limited damage to an individual, organisation or government.**	**Valuable, important and sensitive information.** Compromise of PROTECTED information would be expected to cause **damage to the national interest, organisations or individuals.**	**Very valuable, important and sensitive information**. Compromise of SECRET information would be expected to cause **serious damage to the national interest, organisations or individuals.**	**The most valuable, important and sensitive information.** Compromise of TOP SECRET information would be expected to cause **exceptionally grave damage to the national interest, organisations or individuals.**
Potential impact on individuals from compromise of the information					
Dignity or safety of an individual (or those associated with the individual)	Information from routine business operations and services. Includes personal information as defined in the *Privacy Act*.[i] This may include information (or an opinion) about an identifiable individual (eg members of the public, staff etc) but would not include information defined as sensitive information under the *Privacy Act*.	Limited damage to an individual is: a. potential harm, for example injuries that are not serious or life threatening or b. discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is **not life threatening**.	Damage to an individual is discrimination, mistreatment, humiliation or undermining of an individual's dignity or safety that leads to potentially **significant harm or potentially life threatening injury**.	Serious damage is discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to **directly threaten or lead to the loss of life of an individual or small group**.	Exceptionally grave damage is: a. widespread loss of life b. discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly lead to the death of a large number of people.
Potential impact on organisations from compromise of the information					
Entity operations, capability and service delivery	Information from routine business operations and services.	Limited damage to entity operations is: a. a degradation in organisational capability to an extent and duration that, while the **entity can perform its primary functions**, the effectiveness of the functions is noticeably reduced b. minor loss of confidence in government.	Damage to entity operations is: a. a degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform one or more of its primary functions** b. major loss of confidence in government.	Serious damage to entity operations is: a. a severe degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform any of its functions** b. directly threatening the internal stability of Australia.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Entity assets and finances, eg operating budget	Information compromise would result in insignificant impact to the entity assets or annual operating budget.	Limited damage to entity assets or annual operating budget is equivalent to $**10 million to $100 million**.	Damage is: a. substantial financial loss to an entity b. **$100 million to $10 billion** damage to entity assets.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Legal compliance, eg information compromise would cause non-compliance with legislation,[ii] commercial confidentiality or legal professional privilege	Information compromise would not result in legal and compliance issues.	Limited damage is: a. issues of legal professional privilege for communications between legal practitioners and their clients b. contract or agreement non-compliance c. failure of statutory duty d. breaches of information disclosure limitations under legislation resulting in less than two years' imprisonment.	Damage is: a. failure of statutory duty or breaches of information disclosure limitations under legislation resulting in two or more years' imprisonment.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to the compromise of information are assessed as to the level of impact to the national interest.
Aggregated data[iii]	An aggregation of routine business information.	A significant aggregated holding of information that, if compromised, would cause limited damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive information that, if compromised, would cause damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause serious damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause exceptionally grave damage to the national interest, organisations or individuals.
Potential impact on government or the national interest from compromise of the information					
Policies and legislation	Information compromise from routine business operations and services. For example, this may include information in a draft format (not otherwise captured by higher business impact level).	Limited damage to government is impeding the development or operation of policies.	Damage to the national interest is: a. impeding the development or operation of major policies b. revealing deliberations or decisions of Cabinet, or matters submitted, or proposed to be submitted, to Cabinet[iv] (not otherwise captured by higher level business impacts).	Serious damage to the national interest is: a. a severe degradation in development or operation of multiple major policies to an extent and duration that the policies can no longer be delivered.	Exceptionally grave damage to the national interest is the collapse of internal political stability of Australia or friendly countries.
Australian economy	Information from routine business operations and services.	Limited damage to government is: a. undermining the financial viability of one or more individuals, minor Australian-based or owned organisations or companies	Damage to the national interest is: a. undermining the financial viability of a major Australian-based or owned organisation or company	Serious damage to the national interest is: a. undermining the financial viability of an Australian industry sector (multiple major organisations in the same sector)	Exceptionally grave damage to the national interest is the collapse of the Australian economy.

Sub-impact category ↓	OFFICIAL	Sensitive information	Security classified information		
		OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
	1 Low business impact	**2 Low to medium business impact**	**3 High business impact**	**4 Extreme business impact**	**5 Catastrophic business impact**
	The majority of official information created or processed by the public sector. This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in **no or insignificant damage to individuals, organisations or government.**	**OFFICIAL information that due to its sensitive nature requires limited dissemination.** OFFICIAL: Sensitive is not a security classification. It is a dissemination limiting marker (DLM), indicating compromise of the information would result in **limited damage to an individual, organisation or government.**	**Valuable, important and sensitive information.** Compromise of PROTECTED information would be expected to cause **damage to the national interest, organisations or individuals.**	**Very valuable, important and sensitive information**. Compromise of SECRET information would be expected to cause **serious damage to the national interest, organisations or individuals.**	**The most valuable, important and sensitive information.** Compromise of TOP SECRET information would be expected to cause **exceptionally grave damage to the national interest, organisations or individuals.**
		b. disadvantaging a major Australian organisation or company.	b. disadvantaging a number of major Australian organisations or companies c. short-term material impact on national finances or economy.	b. long-term damage to the Australian economy to an estimated total in excess of $20 billion.	
National infrastructure	Information from routine business operations and services.	Limited damage to government is damaging or disrupting state or territory infrastructure.	Damage to the national interest is damaging or disrupting significant state or territory infrastructure.	Serious damage to the national interest is shutting down or substantially disrupting significant national infrastructure.	Exceptionally grave damage to the national interest is the collapse of all significant national infrastructure.
International relations	Information from routine business operations and diplomatic activities.	Limited damage to government is minor and incidental damage or disruption to diplomatic relations.	Damage to the national interest is: a. short-term damage or disruption to diplomatic relations b. disadvantaging Australia in international negotiations or strategy.	Serious damage to the national interest is: a. severely disadvantaging Australia in major international negotiations or strategy b. directly threatening internal stability of friendly countries, leading to widespread instability c. raising international tension or severely disrupting diplomatic relations resulting in formal protest or sanction.	Exceptionally grave damage to the national interest is directly provoking international conflict or causing exceptionally grave damage to relations with friendly countries.
Crime prevention, defence or intelligence operations	Information from routine business operations and services.	Limited damage to government is: a. impeding the detection, investigation, prosecution of, or facilitating the commission of low-level crime b. affecting the non-operational effectiveness of Australian or allied forces without causing risk to life.	Damage to the national interest is: a. impeding the detection, investigation, prosecution of, or facilitating the commission of an offence with two or more years imprisonment b. affecting the non-operational effectiveness of Australian or allied forces that could result in risk to life.	Serious damage to the national interest is major long-term impairment to the ability to investigate or prosecute serious organised crime[v] affecting the operational effectiveness, security or intelligence capability of Australian or allied forces.	Exceptionally grave damage to the national interest is significantly affecting the operational effectiveness, security or intelligence operations of Australian or allied forces.

Table 1 notes:

[i] Section 6 of the *Privacy Act 1988* provides definitions of 'personal information' and 'sensitive information':

'***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.'

'***sensitive information*** means:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

(that is also personal information); or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.'

Where compromise of personal information, especially sensitive information under the Privacy Act would lead to damage, serious damage or exceptionally grave damage to individuals, this information warrants classification.

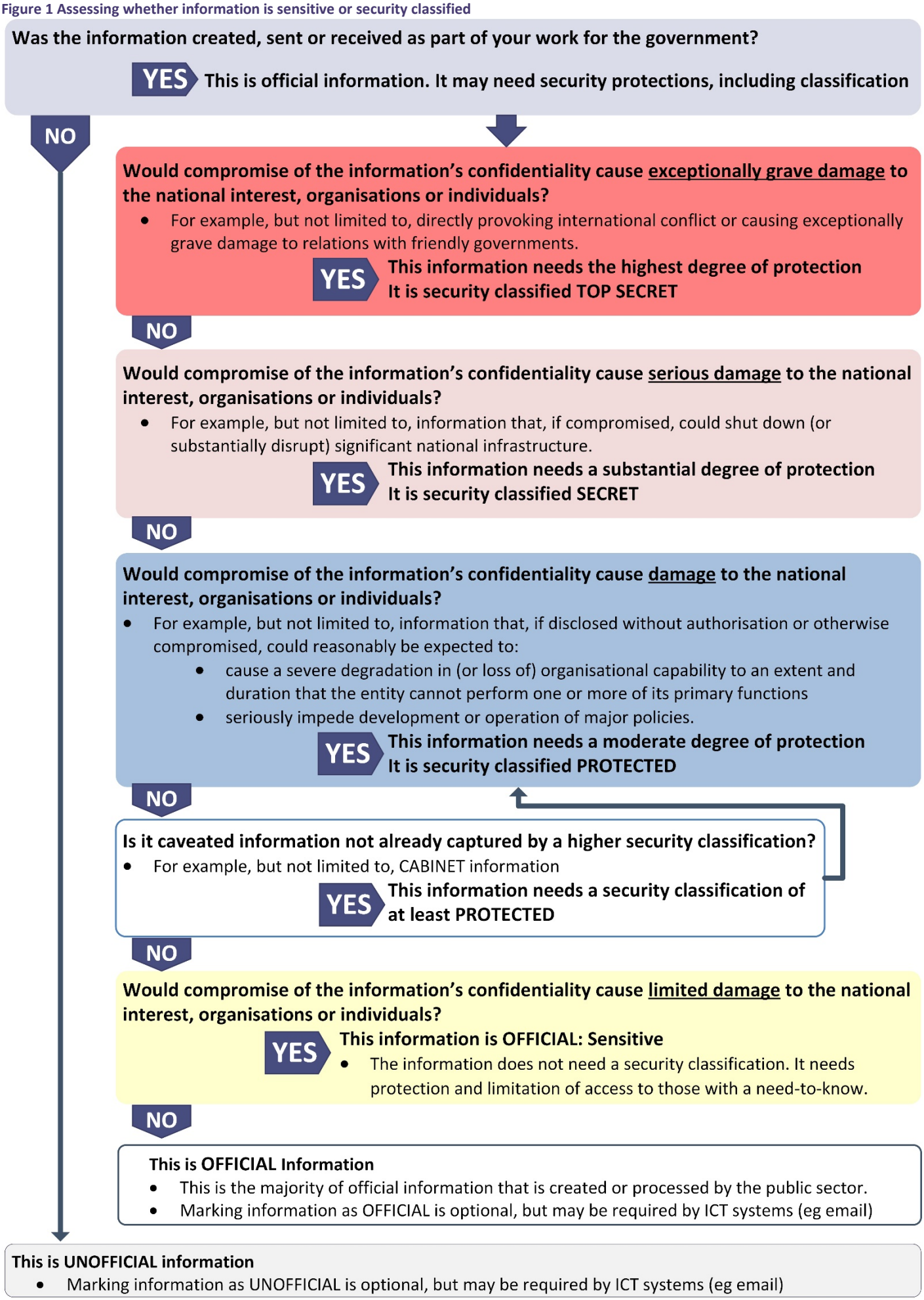
[ii] In its report Secrecy Laws and Open Government in Australia the Australian Law Reform Commission identified 506 secrecy provisions in 176 pieces of legislation, including 358 distinct criminal offences. Examples of legislation including secrecy provisions include: *Social Security Act 1991* and *Social Security (Administration) Act 1999, Taxation Administration Act 1953, Census and Statistics Act 1905*, and, more generally, the *Criminal Code.*

[iii] A compilation of information may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications.

[iv] This includes official records of Cabinet, Cabinet business lists, minutes, submissions, memoranda or matters without submission, and any other information that has been submitted or proposed to be submitted to Cabinet.

[v] Serious organised crime as defined in the Convention Against Transnational Organised Crime.

Figure 1 Assessing whether information is sensitive or security classified



C.2.5 Sanitising, reclassifying or declassifying information

29. **Requirement 3** mandates that the originator of the information remains responsible for controlling the sanitisation, reclassification or declassification of its information. No other entity may change the information's classification unless authorised to do so by the originator.

30. Information may require modification (sanitising) to allow its wider distribution and potential use. Information can be changed to reduce its sensitivity or classification by editing, disguising or altering information to protect intelligence, sources, methods, capabilities, analytical procedures or privileged information. Once sanitised, the information can be declassified or reclassified (see **Table 2**).

Table 2 Definitions reclassification and declassification of information

Term	Definition
Reclassification	The administrative decision to change the security classification of information based on a reassessment of the potential impacts of its compromise. Reclassification may raise or lower the security classification of information.
Declassification	The administrative decision to reduce the security classification of information to OFFICIAL (an unclassified state) when it no longer requires security classification handling protections.

31. The Attorney-General's Department recommends entities establish procedures so that information is automatically declassified:

    a. if the originator set a specific date or event for declassification based on an assessment of the period in which the information might cause damage, when that date or event occurs.

    b. if the originator did not set a specific date or event for declassification, when the open access period under the *Archives Act 1983* commences. For guidance on open access periods, see the National Archives of Australia website.

32. The Attorney-General's Department also recommends entities establish procedures to encourage regular review of classified information for continuing sensitivity (ie if the compromise of the information would still cause damage) using the impact-based classification assessment described in C.2.3 When to assess information sensitivity or security classification. For example, these reviews could be done after a project is completed or when a file is withdrawn from (or returned to) use. Information is declassified or reclassified to a lower classification when a reassessment of its Business Impact Level indicates it no longer meets the original Business Impact Level to which its classification applies.

33. Consistent with **Requirement 4**, information that has been reclassified or declassified must be clearly identified using an applicable protective marking to reflect the new assessment of the Business Impact Level—see C.5.1 Protective markings for sensitive and security classified information.

C.2.6 Historical security classifications

34. There are historical security classifications and other protective markings (eg CONFIDENTIAL classification) that no longer reflect Australian Government policy. For assistance in applying appropriate handling protections (and assessing damage to the national interest, organisations or individuals) to historical classifications, see **Annex F**.

C.3 Caveats and accountable material

35. Certain information may have a caveat in addition to a security classification. The caveat is a warning that the information has special protections in addition to those indicated by the security classification.

36. The Australian Government Security Caveats Guidelines establishes four categories of caveats:

    a. codewords (sensitive compartment information)

    b. foreign government markings

    c. special handling instructions

    d. releasability caveats.

37. **Table 3** describes caveats commonly used across government.

38. Caveats are not classifications and must appear with an appropriate security classification.

39. Accountable material is information that requires the strictest control over its access and movement. Accountable material includes:

    a. TOP SECRET security classified information

    b. some types of caveated information, being:

        i. all codeword information

        ii. select special handling instruction caveats, particularly CABINET information at any security classification

    c. any classified information designated as accountable material by the originator.

40. What constitutes accountable material may vary from entity to entity and could include budget papers, tender documents and sensitive ministerial briefing documents.

41. **Requirement 6** mandates that caveated information and accountable material be clearly marked and handled in accordance with the originator and the caveat holder's special handling requirements as established in the Australian Government Security Caveats Guidelines. These special caveat requirements apply in addition to the classification handling requirements. Additional information about handling caveats is available in the Sensitive Material Security Management Protocol and the Australian Government Security Caveats Guidelines on a need-to-know basis on GovTEAMS.

42. **Requirement 3** requires the originator's approval to remove or change a security classification applied to information. To be consistent with **Requirement 3**, the prior agreement of the originating entity also needs to be obtained to remove a caveat.

Table 3 Caveat types

Caveat types	What kinds of information does this type of caveat cover	What special handling requirements does this caveat impose
Codewords (sensitive compartmented information)	Use of codewords is primarily within the national security community. A codeword indicates that the information is of sufficient sensitivity that it requires protection in addition to that offered by a security classification. Each codeword identifies a special need-to-know compartment. A compartment is a mechanism for restricting access to information by defined individuals who have been 'briefed' on the particular sensitivities of that information and any special rules that may apply. The codeword is chosen so that its ordinary meaning is unrelated to the subject of the information.	It may be necessary to take precautions beyond those indicated by the security classification to protect the information. These will be specified by the entity that owns the information, for instance those with a need to access the information will be given a special briefing first.
Foreign government markings	Foreign government markings are applied to information created by Australian agencies from foreign source information.	PSPF Policy 7: Security governance for international sharing requires that, where an international agreement or international arrangement is in place, entities must safeguard sensitive or security classified foreign entity

Caveat types	What kinds of information does this type of caveat cover	What special handling requirements does this caveat impose
		information or assets in accordance with the provisions set out in the agreement or arrangement. Foreign government marking caveats require protection at least equivalent to that required by the foreign government providing the source information.
Special handling instructions	Use of special handling instructions is primarily within the national security community. Some special handling instructions are used more broadly across government, as follows:	Special handling instructions indicate particular precautions for information handling.
	EXCLUSIVE FOR (named person) The EXCLUSIVE FOR caveat identifies information intended for access by a named recipient only.	Access to EXCLUSIVE FOR information is limited to a named person, position title or designation.
	CABINET The CABINET caveat identifies any information that: a. is prepared for the purpose of informing the Cabinet b. reveals the decision and/or deliberations of the Cabinet c. is prepared by departments to brief their ministers on matters proposed for Cabinet consideration d. has been created for the purpose of informing a proposal to be considered by the Cabinet.	The Cabinet Handbook specifies handling requirements for Cabinet documents. This includes applying a security classification of at least PROTECTED to all Cabinet documents and associated records.
Releasability caveats	There are three releasability caveats used across government:	Releasability caveats limit access to information based on citizenship.
	Australian Eyes Only (AUSTEO) The AUSTEO caveat indicates only Australian citizens can access the information. Additional citizenships do not preclude access.	Information marked AUSTEO is only passed to, or accessed by, Australian citizens. While a person who has dual Australian citizenship may be given AUSTEO-marked information, in no circumstance may the Australian citizenship requirement be waived.
	Australian Government Access Only (AGAO) In limited circumstances, AGAO is used by the: a. Australian Signals Directorate (ASD) b. Australian Security Intelligence Organisation (ASIO) c. Australian Secret Intelligence Service (ASIS) d. Department of Defence e. Office of National Intelligence (ONI).	ASD, ASIO, ASIS, the Department of Defence and ONI may pass information marked with the AGAO caveat to appropriately cleared representatives of Five Eyes foreign governments on exchange or long-term posting or attachment to the Australian Government. For other entities, AGAO information is handled as if it were marked AUSTEO.
	Releasable To (REL) The Releasable To (REL) caveat identifies information that has been released or is releasable to citizens of the indicated countries only. Countries are identified using three letter country codes from International Standard ISO 3166-1:2013 Codes for the representation of names of countries and their subdivisions – Alpha 3 codes.	For example, REL AUS/CAN/GBR/NZL/USA means that the information may be passed to citizens of Australia, Canada, United Kingdom, New Zealand and the United States of America only. The caveat is an exclusive marking that disqualifies a third-party national seconded or embedded in an Australian or foreign government entity from accessing the information.

C.4 Information management markers

43. Information management markers are an optional way for entities to identify information that is subject to non-security related restrictions on access and use. They are subset of the controlled list of terms for the 'Rights Type' property in the National Archives of Australia's Australian Government Recordkeeping Metadata Standard (AGRkMS).

44. Information management markers are not protective markers.

45. The information management markers are described in **Table 4**.

Table 4 Assessing whether to use an information management marker (IMM)

Whether to use an IMM	Which IMM to use	Notes
If the information is subject to legal professional privilege	Use the **legal privilege** IMM – Restrictions on access to, or use of, information covered by legal professional privilege.	Compromise of the confidentiality of information subject to legal professional privilege is likely to cause at least limited damage to the national interest, organisations or individuals. The Attorney-General's Department recommends that the legal privilege IMM only be used with **OFFICIAL: Sensitive or above**.
If the information is subject to one or more legislative secrecy provisions	Use the **legislative secrecy** IMM – Restrictions on access to, or use of, information covered by legislative secrecy provisions.	Compromise of the confidentiality of information subject to legislative secrecy provisions is likely to cause at least limited damage to the national interest, organisations or individuals and the damage may be defined in legislation. The Attorney-General's Department recommends that the legislative secrecy IMM only be used with **OFFICIAL: Sensitive or above**.
If the information is personal information as defined in the *Privacy Act 1988*	Use the **personal privacy** IMM – Restrictions under the Privacy Act on access to, or use of, personal information collected for business purposes.	The Privacy Act requires entities to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure. The Act defines personal information as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'. The Privacy Act also defines 'sensitive information' which includes personal information about an individual's: – racial or ethnic origin – political opinions – membership of a political organisation – religious beliefs or affiliations – philosophical beliefs – membership of a professional or trade organisation or trade union – sexual orientation or practices – criminal record – health or genetic information – some aspects of biometric information The Privacy Act generally affords a higher level of privacy protection to sensitive information than to other personal information. The Attorney-General's Department recommends that the personal privacy IMM only be used with **OFFICIAL: Sensitive or above**.

C.5 Minimum protections for sensitive and security classified information

46. In addition to the following guidance, **Annexes A to D** establish the key operational controls to protect sensitive and security classified information.

47. Consistent with PSPF Policy 2: Management structures and responsibilities Requirement 2, each entity is required to develop and use procedures to cover all elements of protective security, including protecting sensitive and security classified information.

48. The Attorney-General's Department recommends entity personnel consult with their own entity security team for advice on the application of protections for sensitive and security classified information. Entity-specific procedures may require personnel to implement the protections in particular ways or to apply a higher level of protection, in order to meet business needs or to address the entity's security risk environment.

C.5.1 Protective markings for sensitive and security classified information

49. Applying protective markings to security classified or sensitive information indicates that the information requires protection, and dictates the level of protection required. Protective markings help control and prevent compromise of information as they are an easily recognisable way for information users (visually) and systems (such as an entity's email gateway) to identify the level of protection the information requires.

50. **Requirement 4** mandates that the originator clearly identify sensitive and security classified information by using applicable protective markings. **Requirement 5** mandates that entities apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process or communicate sensitive or security classified information.

51. The OFFICIAL marker may be used to identify information that is an Australian Government record that is not sensitive or security classified. Similarly, the UNOFFICIAL marker may be used to identify information generated for personal or non-work related purposes. Use of these markers is not mandatory.

C.5.1.1 Applying text-based protective markings

52. **Requirement 4** indicates text-based protective markings are the preferred method to identify sensitive and security classified information. **Figure 2** Protectively marking physical (printed) information provides an example of applying protective markings.

53. To achieve clearly identifiable protective markings, the Attorney-General's Department recommends:

    a. using capitals, bold text, large font and a distinctive colour (red preferred), for example **OFFICIAL**

    b. placing markings at the centre top and bottom of each page

    c. separating markings by a double forward slash to help clearly differentiate each marking.

54. The order of precedence or hierarchy for protective markings is:

    a. classification (or the OFFICIAL: Sensitive dissemination limiting marker)

    b. foreign government information markings (if any)

    c. caveats or other special handling instructions (if any) then

    d. (optional) information management markers (if any).

55. Paragraph grading indicators are useful where there is a need to identify the security classification of each individual paragraph or section, in addition to the document's overall protective marking or classification. Use of paragraph grading indicators is optional.

56. The Attorney-General's Department recommends that, when used, paragraph grading indicators:

    a. appear in the same colour as the text within the document either in:

        i. brackets at the start or end of each paragraph, or

        ii. the margin adjacent to the first letter of the paragraph.

    b. be written in full or abbreviated by the first letter/s of the markings, as follows:

        i. (UO) for UNOFFICIAL

ii. (O) for OFFICIAL

iii. (O:S) for OFFICIAL: Sensitive

iv. (P) for PROTECTED

v. (S) for SECRET

vi. (TS) for TOP SECRET.

57. The paragraph or section with the most valuable, important or sensitive information (highest classification) dictates the document's overall protective marking or classification.

Figure 2 Protectively marking physical (printed) information

In this example, paragraph 1 contains the most valuable, important and sensitive information in the document. The information in this paragraph dictates the document's overall classification.

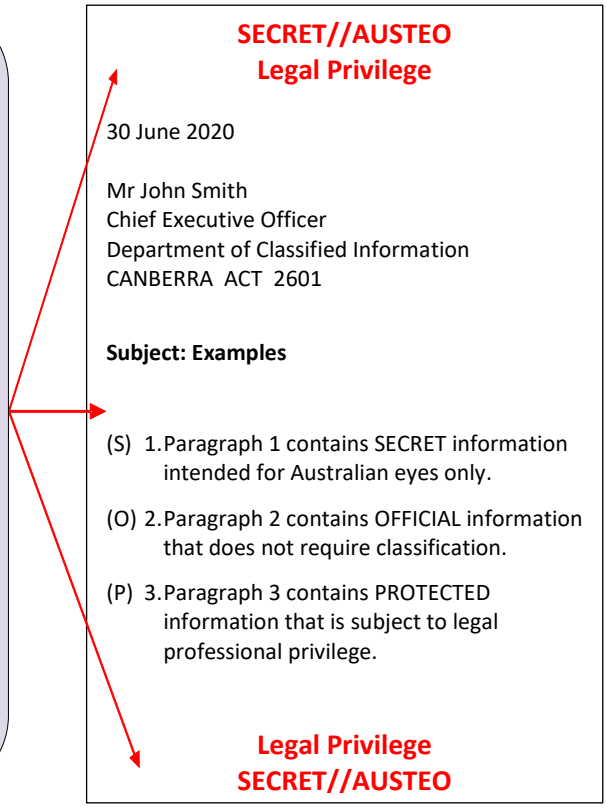
Compromise of the information in paragraph 1 could be expected to cause serious damage to the national interest, organisations or individuals. The information in paragraph 1 is classified as SECRET. This means the document's overall classification is also SECRET.

Additionally, the information in paragraph 1 can only be accessed by Australian citizens and the AUSTEO caveat has been applied. For guidance on caveats, see C.3 Caveats and accountable material .

Paragraph 3 contains information that is subject to legal professional privilege. For guidance on (optional) information management markers, see 0

Information management markers.

To meet the protective marking requirements, the SECRET marking is conspicuously applied to the top and bottom of the page. An AUSTEO caveat marking is also applied. The double forward slash helps to clearly differentiate each marking. As this entity uses the optional information management markers, the legal privilege



C.5.1.2 Applying protective markings if text-based markings cannot be used

58. If text-based markings cannot be used (eg on certain media or assets), **Requirement 4** mandates that colour-based markings must be used. **Annexes A to E** identify the recommended colours to use for a colour-based marking system.

59. Colour-based markings use the RGB model, which refers to Red (R), Green (G) and Blue (B) colours that can be combined in various proportions to obtain any colour in the visible spectrum. **Table 5** specifies the recommended RGB colour-based marking that applies to each security classification. There are no specific RGB colours for OFFICIAL: Sensitive and OFFICIAL information, although a Yellow colour is recommended for OFFICIAL: Sensitive.

Table 5 RGB cell colour for colour-based markings

Security classification	Colour-based marking	RGB cell colour
PROTECTED	Blue	R 79, G 129, B 189
SECRET	Pink/Salmon	R 229, G 184, B 183
TOP SECRET	Red	R 255, G 0, B 0

60. If both text-based and colour-based markings cannot be used (eg for verbal information), entities must use a scheme to identify sensitive and classified information. **Requirement 4** mandates that the scheme must be documented and that entities must train personnel appropriately. For example, a scheme could include an entity policy for meetings that may include discussion of classified information—that participants identify at the commencement of the meeting the level of sensitive or security classified information to be discussed.

61. Other markings, for example entity-specific markings, are not recognised by this policy. A standard set of markings ensures common understanding, consistency and interoperability across systems and government entities. Other markings may confuse users about appropriate handling protections.

C.5.1.3 Applying protective markings through metadata

62. Metadata is a term used for 'data about data'. On ICT systems, text-based protective markings are supplemented by the use of metadata to describe, among other things, key security characteristics of information.

63. For electronic records management systems, the National Archives of Australia produces the AGRkMS to provide standardised metadata terms and definitions for consistency across government. The minimum metadata set is a practical application of the standard that identifies the metadata properties essential for agency management and use of business information. **Requirement 5** mandates that entities apply the AGRkMS metadata properties.

64. From an information security perspective, there are three metadata properties of importance:

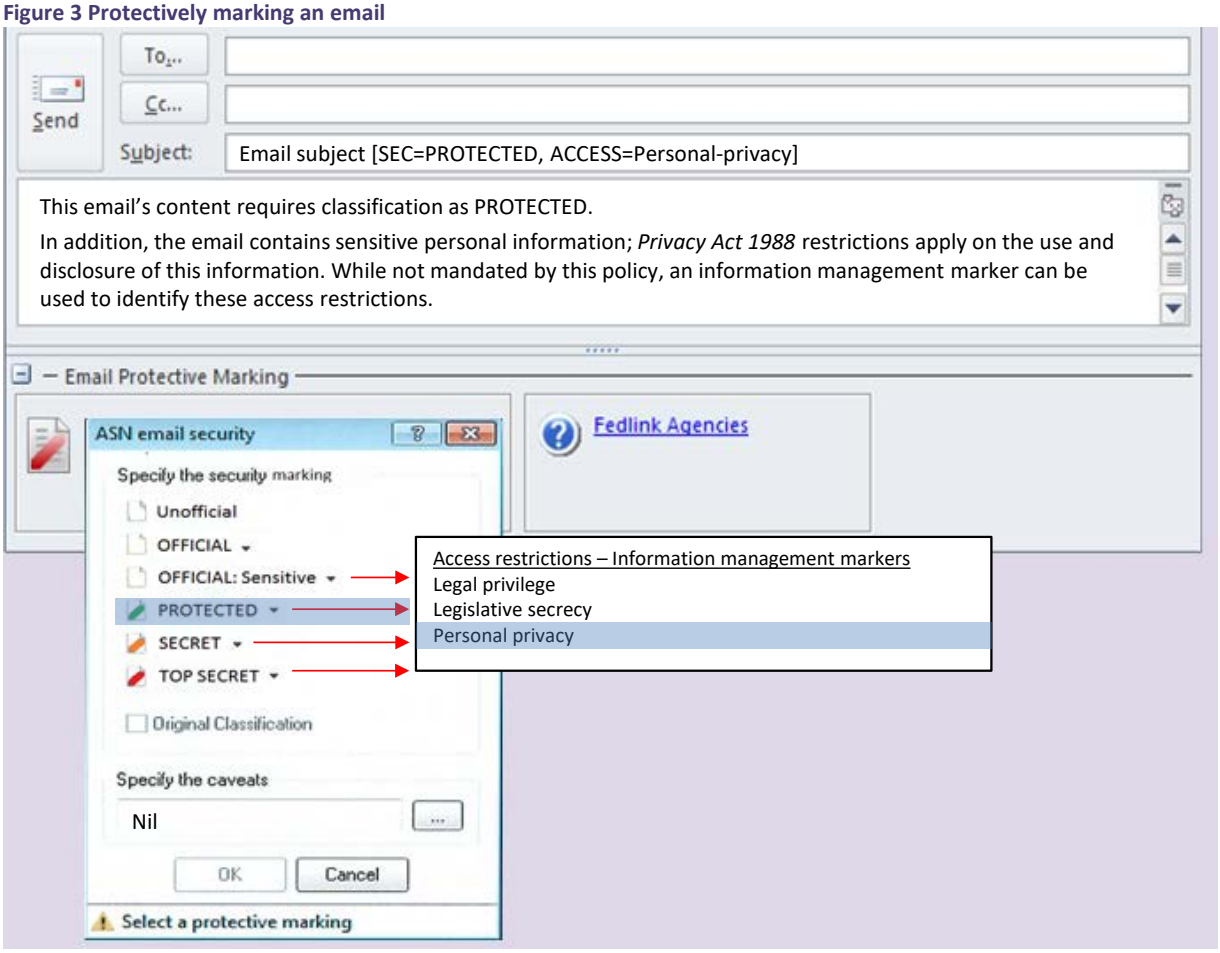
    a. security classification property—identifies the security classification of the information and is used to identify information that is restricted to users with appropriate security clearance permissions. **Requirement 5** mandates application of this property for all classified information

    b. security caveat property—can only be used with the security classification property. Identifies that the security classified information requires additional special handling and that only people cleared and briefed to see it may have access. **Requirement 5** mandates application of this property for caveat information

    c. rights property—optional property to identify non-security related restrictions on the use or access to records. The National Archives of Australia has established a subset of rights property terms for common usage as information management markers to categorise information

65. For emails, the preferred approach is for entities to apply protective markings to the internet message header extension, in accordance with the Email Protective Marking Standard at Annex G. This helps with construction and parsing by email gateways and servers, and allows for information handling based on the protective marking. Where an internet message header extension is not possible, protective markings are placed in the subject field of an email. See **Figure 3** for an example of a protectively marked email.

Figure 3 Protectively marking an email



66. When printed, an email is considered a physical document, as such, a visual presentation of the protective marking (such as a separate line in the email) is important.

C.5.2 Limiting disclosure and access to sensitive and security classified information

67. The vast majority of official information can be shared, where appropriate. The PSPF Policy 9: Access to information states that:

> *Each entity must enable appropriate access to official information. This includes … ensuring that those who access sensitive or security classified information are appropriately security cleared and need to know that information.*

C.5.2.1 Limiting by need-to-know principle

68. PSPF Policy 9: Access to information establishes that the need-to-know principle applies for all access to sensitive and security classified information. Limiting access by staff and others (eg contractors) to information on a need-to-know basis guards against the risk of unauthorised access or misuse of information. Personnel are not entitled to access information merely because it would be convenient for them to know or because of their status, position, rank or level of authorised access.

69. The Attorney-General's Department recommends that entities consider staff access to OFFICIAL information on a need-to-know basis, although this is not a requirement of the PSPF.

C.5.2.2 Limiting by security clearance level

70. PSPF Policy 9: Access to information establishes the level of security clearance required to access sensitive and security classified information. This requirement is restated in **Annexes A to D**.

71. For further guidance on obtaining personnel security clearances see PSPF Policy 12: Eligibility and suitability of personnel.

C.5.2.3 Keeping records of disclosure and access

72. Monitoring and auditing the dissemination of information plays an important role in information protection.

73. For highly classified or caveated information (such as TOP SECRET information or accountable material), it is critical to maintain an auditable register (such as a Classified Document Register) of all incoming and outgoing information and material, transfers or copying, along with regular spot check audits. Personnel can conduct spot check audits by sighting documents listed in the register and documenting the process (eg counter-signing the register).

74. The Attorney-General's Department recommends that entities:

    a. keep an audit log or register for documents at other classification levels (particularly for SECRET information), or registered information received from other entities.

    b. develop procedures for regular spot checks to ensure accountable material (including TOP SECRET information) is accounted for and being handled, used and stored appropriately. For example, do a spot check of 5 per cent of TOP SECRET files per month, with 100 per cent of TOP SECRET files checked within a two-year period

    c. use receipts for transfer of all security classified information. Receipts can be used to identify the date and time of dispatch, the dispatching officer's name and a unique identifying number. Additionally, receipts can be used as a mechanism to control the incoming transfer of information (eg a two-part receipt placed in the inner envelope with the information means the addressee can keep one portion and sign and return the other to the sender).

75. There may be other legislative requirements for record keeping. For example, under the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, a Privacy Officer is required to maintain a record of an entity's personal information holdings and a register of privacy impact assessments.

76. Markings such as page and reference numbering can be used to identify and track classified information. There may be other reasons to use reference markings, for example **Requirement 6** mandates the use of page and reference numbering for all accountable material, even if it is not sensitive or classified.

C.5.3 Using sensitive and security classified information

77. It is a core requirement of this policy that entities 'implement operational controls for their information holdings, proportional to their value, importance and sensitivity'. Consistent with this requirement, PSPF Policy 15: Physical security for entity resources, mandates that:

> *Each entity must implement physical security measures that minimise or remove the risk of…information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.*

78. When sensitive and security classified information is being 'used'—able to be read, viewed, heard or comprehended—it may be at higher risk of compromise. Different physical environments pose different risks for information compromise.

79. Entities can minimise risk through the application of operational controls, complementing the physical security measures required under PSPF Policy 15. The Attorney-General's Department recommends entities establish procedures that facilitate personnel maintaining good security practices while using sensitive and security classified information, including:

a. maintaining *awareness* of their environment, including who will or could access, use or remove information for which the officer is responsible and whether they could be exposed to information they are not authorised to access.

b. exercising *judgement* to assess environmental suitability

c. taking *appropriate steps* to minimise the risk of an unauthorised person accessing, using or removing the information.

d. employing appropriate *physical handling* of information, for example when carrying or when the information is not in active use.

80. **Annexes A to D** establish the physical security zones where different levels of sensitive and security classified information can be used.

C.5.3.1 Using information when working away from the office

81. Working away from the office is all work undertaken by personnel away from entity facilities, including using mobile computing and communications and by teleworkers. PSPF Policy 15: Physical security for entity resources recommends that when personnel are working away from the office:

> *…entities consider the security risks of the environments in which their personnel operate, the type of information that will be used and how that information will be accessed.*

Relevant definitions

Use: Information is in **use** if it can be read, viewed, heard or comprehended by a person.

Entity facility: An entity facility means the physical security zones of an Australian agency or department, and includes Australian Government embassies, high commissions and consulates

Teleworkers: personnel with remote ICT access in a fixed location.

Regular ongoing home-based work: is where an arrangement exists between an individual and their agency/manager for them to work from home on an ongoing basis. Any other work done at home is **occasional home-based work**.

82. The Attorney-General's Department's recommendations for maintaining good security practices when using sensitive and security classified information in an entity facility (C.5.3 Using sensitive and security classified information) are also relevant where sensitive and security classified information is used when working away from the office.

83. Business requirements may mean personnel need to use or store sensitive or security classified information in:

a. other entities' facilities (eg to attend a meeting)

b. alternative office spaces (eg another entity's facility, state or territory government facilities, allied secure and accredited facilities)

c. private homes (eg for regular ongoing home-based work or occasional home-based work)

d. public spaces (eg public transport, cafés, restaurants, hotels and transit lounges) within Australia

e. facilities overseas (eg to attend a meeting with foreign country officials).

84. In some situations, for practical reasons personnel may need to hold the information for a period of time before reaching the location in which they will use the information—for example, taking information home the night before an early meeting or early travel to another city within Australia.

85. The officer who removes sensitive or security classified information from a security zone is the responsible officer. The responsible officer has custody of the information and is responsible for handling the information in accordance with the minimum protections for the classification. **Annexes A to D** establish the minimum protections for using sensitive and security classified information outside the entity's facility, including outlining information that may not be taken out of entity facilities.

86. Where the responsible officer:

a. needs to store sensitive and security classified information outside an entity facility, the guidance at C.5.4 Storing sensitive and security classified information applies

b. needs to carry sensitive and security classified information from one location, to use at a second location (for example, from their entity facility to use at home or to attend a meeting in another entity's facility), the guidance at C.5.5 Carrying sensitive and security classified information applies

c. needs to transfer sensitive and security classified information to another individual, the guidance at C.5.6 Transferring and transmitting sensitive and security classified information applies.

C.5.3.2 Using information on mobile computing and communications

87. Mobile computing and communications encompasses work using computing and communications devices such as laptops, notebooks, tablets, smart mobile phones and personal digital assistants. Given their portable nature, these mobile devices provide a platform for entity mobility by enabling personnel to use, store and communicate sensitive and classified information away from the traditional desktop environment.

88. The Attorney-General's Department's recommendations for maintaining good security practices when using sensitive and security classified information in an entity facility (C.5.3 Using sensitive and security classified information) are also relevant where sensitive and security classified information is being used via a mobile device, whether within or outside an entity facility. Similarly, the guidance at C.5.4 Storing sensitive and security classified information applies.

89. **Annexes A to D** establish the minimum protections for accessing, storing or communicating sensitive and security classified information on mobile devices.

90. The Attorney-General's Department recommends entities ensure that use of privately-owned mobile devices do not present an unacceptable security risk.

91. For more detailed guidance on using mobile devices, including granting access to government information or systems by personal (or privately-owned) mobile devices, see the Australian Government Information Security Manual.

C.5.3.3 Using information on official travel outside Australia

92. Special care is necessary when sensitive or security classified information (physical or held on a mobile device) is removed from entity facilities for use outside Australia.

93. The Attorney-General's Department recommends entities establish entity procedures to:

a. consider country-specific advice

b. if required, consult with the Department of Foreign Affairs and Trade (DFAT) for practical advice, including on the availability of transfer and storage options using resources available through Australian Government embassies, high commissions and consulates, and

c. authorise officers to travel with sensitive and security classified information.

94. **Annexes A to D** establish the minimum protections for travelling with sensitive and security classified information outside Australia.

C.5.4 Storing sensitive and security classified information

95. When sensitive and security classified information is unattended (ie it is not under the immediate control or in the physical presence of the person responsible for it), **Requirement 7** mandates entities ensure the information is stored securely in an appropriate security container for the approved zone. Securely storing sensitive and security classified official information protects the information from compromise.

96. **Requirement 7** also applies to mobile devices holding sensitive and security classified information. These items may also need protections as a valuable asset (see PSPF Policy 15: Physical security for entity resources). The Attorney-General's Department recommends that mobile devices be stored in a secured state, where encryption is active when the device is not in use. The Australian Government Information Security Manual includes guidelines on encryption for mobile devices.

Explanation of mobile device storage encryption

A mobile device is in a **secured state** if appropriate encryption is active when the device is not in active use. The Australian Government Information Security Manual includes guidelines on encryption for mobile devices.

In all other circumstances–when the device is in use or is deemed to be in use because encryption is not active or does not meet the standard prescribed in the ISM–the device is in an **unsecured state.**

97. The National Archives of Australia Australian Government Information Management Standard requires that entities store information securely and preserve it in a usable condition for as long as required for business needs and community access. In accordance with the Information Management Standard, a secure and suitable storage environment is one that prevents unauthorised access, duplication, alteration, removal and destruction.

98. Ways to minimise duplication or alteration of information include:

    a. reproducing sensitive or security classified information only when necessary

    b. immediately destroying spare or spoilt copies (such destruction is defined as 'normal administrative practice' in the Archives Act 1983 and does not need specific permission from the National Archives of Australia). For guidance on destroying sensitive and security classified information, see C.5.7.1 Destroying sensitive and security classified information.

99. **Annexes A to D** establish the minimum protections for storing sensitive and security classified information and mobile devices holding information. For guidance on physical security zones, see the PSPF Policy 16: Entity facilities.

C.5.4.1 Clear desk, session and screen locking procedures

100. The Attorney-General's Department recommends entities establish clear desk, session and screen locking procedures. These procedures are an additional way to protect information when unattended. These procedures promote awareness of the requirements to protect information from compromise and assist entity personnel to secure all files, documents (electronic as well as paper), sensitive and classified material (including portable and attractive items, for example iPads, mobile phones, memory sticks, PDAs etc) and other official information in their custody.

101. The Attorney-General's Department recommends entities' procedures prompt personnel to ensure that:

    a. no sensitive or security classified information is left unattended on a desk (ie it is stored appropriately)

    b. ICT equipment (computers and media devices) is locked when not in use

    c. electronic media and devices containing classified or sensitive information are secured

    d. all portable and attractive items are secured

    e. keys to classified storage devices are secured

    f. keys are not left in doors and drawers (at the end of the day or for an extended period of time).

102. For further information on applying session and screen locking procedures, see the Australian Government Information Security Manual.

C.5.5 Carrying sensitive and security classified information

103. It is important to implement effective protections when carrying sensitive and security classified information from one location to use in another location, including to attend meetings inside entity facilities, outside and between entity facilities. Higher levels of protection are required if sensitive or security classified information is carried through a less secure zone (eg carrying SECRET material through a Zone 1 or carrying TOP SECRET information through a Zone 1 or Zone 2) or outside the entity in public spaces.

104. **Annexes A to D** outline the minimum protections for carrying each level of sensitive and security classified information, including for carrying outside entity facilities and between entity facilities.

105. ASIO-T4 and the Security Construction and Equipment Committee (SCEC) provide advice on security equipment for protecting classified information while carrying it. This includes advice on SCEC-endorsed tamper evident seals and packaging, as well as guidance on selecting briefcases suitable for the carriage of security classified information. The advice is available on the Protective Security Policy GovTEAMS community.

106. For guidance on transferring information to another person or entity, see C.5.6 Transferring and transmitting sensitive and security classified information.

C.5.6 Transferring and transmitting sensitive and security classified information

107. **Requirement 8** mandates that entities ensure sensitive and security classified information is transferred and transmitted by means that deter and detect compromise.

108. Examples of transferring information include:

a. handing information to a person within an office environment (ie within entity facilities)

b. sending information through the entity's internal mail to a person who works in the same building

c. sending information through the entity's internal mail to a person who works in a different building

d. handing or sending information to a person in another entity

e. giving a person a secure approved USB or other storage device that holds the information.

109. Examples of transmitting information include:

a. emailing information to a person within the entity or in a different entity

b. verbally communicating information to a person within the entity or another entity (eg by telephone or videoconference).

110. To ensure sensitive and security classified information is only transferred or transmitted to people with a need-to-know, entities are encouraged to identify information recipients by:

a. a specific position, appointment or named individual

b. where physical information is being transferred:

i. a full location address (eg not a post office box for physical delivery, as this may be unattended)

ii. an alternative individual or appointment where relevant (eg for TOP SECRET information).

c. where information is being electronically transmitted, an email address exclusive to those individuals with a need-to-know (eg not a mailbox with unrestricted access).

C.5.6.1 Transferring physical sensitive and security classified information

111. When transferring physical sensitive and security classified information, the Attorney-General's Department recommends adopting security measures to:

a. obscure that the information is sensitive or security classified

b. deter and detect unauthorised access to the information.

112. The security measures required to protect sensitive and security classified information and caveated information and material during physical transfer depend on the sensitivity or security classification level of the information, where the information is going from and to, and the transfer method used.

113. **Annexes A to D** establish the minimum protections to transfer each level of sensitive and security classified information. Where transfer is between physical locations:

    a. a tamper-evident double barrier is used to protect security classified information. The most common method to achieve this is 'double-enveloping'

    b. a secure transfer method is used, such as by entity safe hand or safe hand by an endorsed courier.

114. It may also be appropriate or required for entities to follow record-keeping procedures when transferring sensitive and security classified information, such as use of receipts.

115. The PSPF does not impose requirements for the transfer of OFFICIAL information (as opposed to OFFICIAL: Sensitive information). The Attorney-General's Department recommends entities ensure that OFFICIAL information is transferred by means which deter and detect compromise (see **Annex E**).

Explanation of double enveloping

'Double enveloping' consists of:

- a tamper evident inner barrier to detect unauthorised access
- an outer barrier to obscure the information's sensitivity or classification and deter unauthorised access.

The inner 'envelope' can consist of:

- an envelope or pouch sealed with a Security Construction and Equipment Committee (SCEC)-approved tamper evident seal so that any tampering is detected, or
- a SCEC-approved single use envelope.

The Attorney-General's Department recommends marking the classification conspicuously on the inner envelope (eg at the top and bottom of the front and back of the envelope).

The outer 'envelope' is some form of sealed opaque covering. It could be a regular mail envelope, a SCEC-approved single-use outer envelope, security briefcase, satchel, pouch or transit bag. It may display information identifying the recipient and any receipt or reference numbers, if required. The Attorney-General's Department recommends avoiding displaying any details on the outer envelope (such as protective markings) that indicate that the information is sensitive or security classified information.

Explanation of safe handing

'Safe hand' means information is dispatched to the addressee in the care of an authorised person or succession of authorised people who are responsible for its carriage and safekeeping. The authorised person could be the responsible officer who removes the information from the entity facility. An authorised person could also be an endorsed courier. 'Entity safe handing' is where all of the authorised persons in the chain are officers of the entity dispatching the information.

Sending information via safe hand establishes an audit trail that provides confirmation that the addressee received the information and helps to ensure the item is transferred in an authorised and secure facility or vehicle. To deter and detect any information tampering, at each handover, a receipt is obtained showing (at a minimum) the identification number, the time and date of the handover, and the name and signature of the recipient.

Sending information via safe hand requires:

- a unique identification number; generally, this will be a receipt number
- that information be in a security briefcase (see the SCEC-Security Equipment Guide on Briefcases for the carriage of security classified information on GovTEAMS) or an approved mailbag (for information, see the SCEC-approved security equipment evaluated product list)
- that information be retained in personal custody.

Safe hand via an endorsed courier

Using an endorsed courier provides a level of assurance for the confidentiality of information being transferred, where it is not possible to use entity personnel to carry the information. This method of transfer is not suitable for protecting valuable or attractive assets such as pharmaceuticals or money. Special arrangements, such as armed escorts may be necessary in certain circumstances.

A number of commercial courier companies have been endorsed by SCEC to provide safe hand courier services. Contact ASIO-T4 by email t4ps@t4.gov.au or see the ASIO-T4 Protective security circular (PSC) 172 (available on a need-to-know basis on GovTEAMS) for advice on SCEC-endorsed safe hand courier services.

Special handling requirements may apply to caveated information. This may preclude the use of a commercial safe hand courier when using certain caveats. For guidance on caveats, see C.3 Caveats and accountable material.

C.5.6.2 Using devices to transfer or transmit sensitive and security classified information

116. Devices that are able to store and communicate information, such as laptops, notebooks, tablets, smart mobile phones, personal digital assistants and USBs, can be used to both transfer and transmit information. Ways to deter and detect information compromise and unauthorised access when devices are used include password protection, encrypting information at rest and remote wiping capabilities.

117. Where devices cannot be protected by these means, the Attorney-General's Department recommends entities apply the protections used for physical information (see C.5.6.1 Transferring physical sensitive and security classified information).

118. Where a device is being used to transfer sensitive and security classified information to another entity—ie the device will be retained by the receiving entity—it may be appropriate for entities to consider additional controls such as receipts (see C.5.2.3 Keeping records of disclosure and access). For guidance on protecting information on ICT systems, see PSPF Policy 11: Robust ICT systems.

C.5.6.3 Transferring sensitive or security classified information outside Australia

119. Special care is necessary when transferring sensitive or security classified information (physical or held on a storage device) outside Australia.

120. **Annexes A to D** establish the minimum protections for transferring sensitive and security classified information outside Australia, including outlining information that may not be transferred outside Australia.

121. The Attorney-General's Department recommends entities:

a. consider country-specific advice

b. check with the Department of Foreign Affairs and Trade (DFAT) about the most appropriate method to transfer sensitive and security classified information outside Australia

c. establish entity procedures if overseas transfers form a routine part of their business.

C.5.6.4 Electronically transmitting sensitive and security classified information

122. Entities electronically transmit information when it is sent or communicated over the internet, through a secure network infrastructure (ie official, PROTECTED, SECRET or TOP SECRET networks) or over public network infrastructure and unsecured spaces. Examples of electronical transmission include using email, facsimile, instant messaging services, GovTEAMS, telephone and videoconference.

123. Information is at increased risk when electronically transmitted, particularly when information is transmitted outside of a controlled environment (eg when an entity does not have control over the entire transmission network).

124. Encryption can be used to assist in protecting information from compromise where insufficient physical security is provided for the protection of information communicated over network infrastructure.

125. Where the electronic transmission involves verbal communication (such as telephone or videoconference), the Attorney-General's Department's recommendations for maintaining good security practices when using sensitive and security classified information are relevant (C.5.3 Using sensitive and security classified information).

126. **Table 6** outlines the minimum protections to deter and detect compromise when transmitting information electronically. For detailed guidance on protecting transmissions over networks, including information on cryptography, see the Australian Government Information Security Manual.

Table 6 Minimum network and encryption levels for transmitting information electronically

Classification/marking	Minimum protections
TOP SECRET (and SECRET Codeword)	a. Communicate information over TOP SECRET secure network. b. Use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information for any communication that is not over a TOP SECRET network.
SECRET	a. Communicate information over SECRET secure networks (or networks of higher classification). b. Use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information for any communication that is not over a SECRET network or network of higher classification.
PROTECTED	a. Communicate information over PROTECTED networks (or networks of higher classification).

Classification/marking	Minimum protections
	b. Encrypt PROTECTED information for any communication that is not over a PROTECTED network or network of higher classification.
OFFICIAL: Sensitive	Communicate information over OFFICIAL networks (or networks of higher classification). Encrypt OFFICIAL: Sensitive information transferred over public network infrastructure, or through unsecured spaces (including Zone 1 security areas), unless the residual security risk of not doing so has been recognised and accepted by the entity. An entity may wish to consider other security measures or mitigating protections already in place, such as: a. validating the recipient's address before sending information in an unencrypted form b. sending sensitive information or large amounts of non-sensitive information as an encrypted or password protected attachment. Australian Privacy Principle 11 imposes additional obligations regarding the transmission of 'personal information' (as defined under the *Privacy Act 1988*); the Office of the Australian Information Commissioner's Guide to Securing Personal Information provides guidance on the reasonable steps that entities may be required to take under the Privacy Act to protect the personal information they hold, including when such information is being transferred or transmitted.
OFFICIAL	a. Communicate information over public network infrastructure or through unsecured spaces (including Zone 1 security areas). b. Encryption recommended.

127. While encryption of OFFICIAL information (as opposed to OFFICIAL: Sensitive information) is not a mandated requirement, entities are required to implement operational controls for all information holdings proportional to their value, importance and sensitivity. The Attorney-General's Department recommends entities ensure that OFFICIAL information is transmitted by electronic means which deter and detect compromise, including use of encryption to assist in protecting OFFICIAL information.

C.5.7 Disposing of sensitive and security classified information

128. Not all information and records are kept forever. Information is managed for as long as it has business value; some information will have long-term historical and social value. **Requirement 9** mandates that entities dispose of sensitive and security classified information in a secure manner. The careless disposal of classified or sensitive information is a serious source of leakage of information and can undermine public confidence in the Australian Government.

129. The National Archives of Australia's Information Management Standard Principle 6 states:

> *Keep business information for as long as required after which time it should be accountably destroyed or transferred.*
>
> *Assess business information against current records authorities to determine which information can be destroyed or transferred.*
>
> *Confirm that there is no need to keep business information beyond the authorised retention period. Examples of needs to keep business information longer include:*
>
> - *anticipated requests for access*
> - *likely legal action*
> - *a significant increase in public interest in the topic*
> - *a disposal freeze issued by the Archives for business information on that issue or event.*

130. Under the Archives Act information disposal includes:

a. its destruction

b. the transfer of its custody or ownership, or

c. damage or alteration.

131. Section 26 of the Archives Act prohibits altering records that are over 15 years old without authorisation from the National Archives.

132. Information disposal includes the: physical destruction of paper records; destruction of electronic records including deleting emails, documents or other data from business systems; transfer of records to another entity as the result of machinery of government changes; and transfer to the National Archives of Australia.

133. Under Section 24 of the Archives Act, information disposal can only take place when it is:

a. approved by the National Archives of Australia

b. required by another law, or

c. part of normal administrative practices that the National Archives of Australia does not disapprove.

134. For guidance, see the National Archives of Australia website, Dispose of information.

C.5.7.1 Destroying sensitive and security classified information

135. A variety of methods can be used for the secure destruction of information in physical form.

136. ASIO-T4 approves specifications for equipment used to destroy security classified information. Commonly used destruction methods include:

a. pulping

b. burning

c. pulverising using hammermills

d. disintegrating by cutting and reducing the waste particle size

e. shredding using crosscut shredders (strip shredders are not approved for destruction of security classified information).

137. The Australian Government Information Security Manual provides guidance on sanitisation and destruction of ICT equipment and storage media. Methods for destroying digital information include:

a. digital file shredding

b. degaussing by demagnetising magnetic media to erase recorded data

c. physical destruction of storage media through pulverisation, incineration or shredding ()

d. reformatting, if it can be guaranteed that the process cannot be reversed.

138. Commercial providers may be used to destroy security classified information. The Attorney-General's Department recommends that entities review the appropriateness of a commercial provider's collection process, transport, facility, procedures and approved equipment when considering external destruction services. These considerations can be made against ASIO-T4 Criteria – agency-assessed and approved destruction service (available on a need-to-know basis on GovTEAMS). Appropriate procedures include ensuring:

a. classified information is attended at all times and the vehicle and storage areas are appropriately secured

b. that destruction is performed immediately after the material has arrived at the premises

c. that destruction of classified information is witnessed by an entity representative

d. destruction service staff have a security clearance to the highest level of security classified information being transported and destroyed, or appropriately security cleared entity staff escort and witness the destruction.

139. A number of commercial providers hold National Association for Information Destruction AAA certification for destruction service (with endorsements as specified in PSC 167 External destruction of security classified information – available on a need-to-know basis on GovTEAMS). These commercial providers are able to destroy security classified information.

140. The Attorney-General's Department recommends information classified TOP SECRET or accountable material be destroyed within entity premises; the originating entity may request notification of destruction. The originator of some accountable material may apply special handling conditions that prevent information destruction being contracted out.

141. While **Requirement 9** mandates that sensitive and security classified information is disposed of securely, this policy does not impose security requirements for how destruction of OFFICIAL: Sensitive information is to occur and **Requirement 9** does not apply to OFFICIAL information. The Attorney-General's Department recommends entities establish procedures for the secure disposal of OFFICIAL and OFFICIAL: Sensitive information.

142. There may be other legislative requirements that apply to the disposal of information. For example, Australian Privacy Principle 11.2 imposes obligations on the destruction and de-identification of personal information under the Privacy Act.

C.6 What to do in the case of an emergency, breach or security violation involving classified information

143. Exceptional situations or emergencies may arise that prevent application of this policy. The PSPF Policy 5: Reporting on security requires entities to report details about exceptional circumstances that affect an entities ability to fully implement this policy and indicate the measures taken to mitigate or otherwise manage identified security risks. The PSPF Policy 5: Reporting on security also mandates that affected entities are advised of any unmitigated security risks.

144. Any compromise of any classified information is considered a security incident. The PSPF Policy 2: Management structures and responsibilities requires entities to investigate, respond to and report on security incidents.

145. In line with this, the Attorney-General's Department recommends entities report:

a. any compromise of classified information to the information's originator as soon as practicable

b. matters relating to national security (such as compromise of SECRET or TOP SECRET information) to the Director-General, Australian Security Intelligence Organisation.

D. Find out more

146. Other legislation and policies that may be relevant to the handling of official government information include the:

a. Archives Act and supporting Commonwealth records management policies such as:

   i. National Archives of Australia Information Management Standard

   ii. National Archives of Australia Digital Continuity 2020 policy

b. Australian Government Information Security Manual

c. Privacy Act and the Office of the Australian Information Commissioner Guides and APP guidelines.

Annex A. Minimum protections and handling requirements for TOP SECRET information

BIL 5	TOP SECRET—exceptionally grave damage to the national interest, organisations or individuals
Protective marking	Apply text-based protective marking **TOP SECRET** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For TOP SECRET a red colour is recommended. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. If marking paragraphs, it is recommended that TOP SECRET is written in full or abbreviated to (TS) and placed either in brackets at the start or end of the paragraph or in the margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle applies to all TOP SECRET information. Ongoing access to TOP SECRET information requires a Negative Vetting 2 security clearance or above. Any temporary access must only be provided to personnel with at least a Negative Vetting 1 security clearance and must be must be supervised.
Use	TOP SECRET information can only be used in Zones 3-5. **Outside entity facilities (including at home)** **Do not** use outside entity facilities (including at home).
Storage	**Do not** leave TOP SECRET information, or a mobile device that processes, stores or communicates TOP SECRET information, unattended. Store securely when unattended. When storing TOP SECRET information, or a mobile device that processes, stores or communicates TOP SECRET information: a. inside entity facilities: i. Zone 5, store in Class B container ii. Zones 3-4, store in exceptional circumstances only for a maximum of 5 days, Zone 4 (in Class B container) or Zone 3 (in a Class A container). b. outside entity facilities: **do not** store TOP SECRET information, or a mobile device that processes, stores or communicates TOP SECRET information, outside entity facilities (including at home).
Carry	When carrying physical TOP SECRET information **always retain it in personal custody** a. inside entity facilities: i. Zones 3-5, in an opaque envelope or folder that indicates classification ii. Zones 1-2, **not recommended**, if required, in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: **not recommended**, if required: i. obtain written manager approval, and ii. place in tamper-evident packaging within a security briefcase, pouch or satchel. Mobile devices that that process, store or communicate TOP SECRET information require explicit approval by the Australian Signals Directorate (ASD). When carrying an approved TOP SECRET mobile device **always retain it in personal custody** a. inside entity facilities: i. Zones 3-5, carry in secured state; if in an unsecured state apply entity procedures ii. Zones 1-2, carry in a secured state; if in an unsecured state, place inside a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities – **not recommended**, if required: i. obtain written manager approval, and

	ii. carry in a secured state; if in an unsecured state, place in tamper-evident packaging within a security briefcase, pouch or satchel.
Transfer	When transferring physical TOP SECRET information a. inside entity facilities i. Zones 3-5, transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if in close proximity and the office environment presents low risk of unauthorised viewing ii. Zones 1-2, transfer by hand or entity safe hand and apply requirements for carrying with written manager approval. b. to another officer in a different facility i. obtain written manager approval ii. apply requirements for carrying outside entity facilities (including using tamper evident packaging), and iii. transfer by hand, entity safe hand, safe hand courier rated BIL 5, or DFAT courier. Any transfer requires a receipt.
Transmit	When transmitting electronically, communicate information over TOP SECRET secure networks. Use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information for any communication that is not over a TOP SECRET network.
Official travel	TOP SECRET information and mobile devices that process, store or communicate TOP SECRET information **must not** be stored or used outside appropriate entity facilities. **Travel in Australia** Travelling domestically with physical TOP SECRET information is **not recommended**, if required: a. obtain written manager approval b. apply requirements for carrying outside entity facilities and any additional entity procedures, and c. for airline travel, retain as carry-on baggage and **do not travel** if the airline requires it to be checked at the gate. **Do not** leave TOP SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility. Travelling domestically with a mobile device that processes, stores or communicates TOP SECRET information is **not recommended**, consider alternative options to access information at destination. If required: a. obtain written manager approval b. apply requirements for carrying outside entity facilities and any additional entity procedures, and c. for airline travel, retain as carry-on baggage; if airline requires carry-on baggage to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim as soon as possible. **Do not** leave device unattended. **Do not** store device while travelling (eg in a hotel room). If storage required, store in an Australian entity facility. **Travel outside Australia** **Do not** travel overseas with TOP SECRET information or a mobile device that processes, stores or communicates TOP SECRET information, seek DFAT advice on options to access information or mobile devices at overseas destination. If access to TOP SECRET information or mobile device provided at overseas destination: a. apply requirements for carrying outside entity facilities and any additional entity procedures, and b. retain in personal custody or store in an Australian entity facility. **Do not** leave TOP SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility.
Disposal	Dispose of TOP SECRET information using a Class A shredder – supervise and document destruction

Annex B. Minimum protections and handling requirements for SECRET information

BIL 4	SECRET—serious damage to national interest, organisations or individuals
Protective marking	Apply text-based protective marking **SECRET** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For SECRET a salmon pink colour is recommended. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. If marking paragraphs, it is recommended that SECRET is written in full or abbreviated to (S) and placed either in brackets at the start or end of the paragraph or in the margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle applies to all SECRET information. Ongoing access to SECRET information requires a Negative Vetting 1 security clearance or above. Any temporary access must be supervised.
Use	SECRET information and mobile devices that process, store or communicate SECRET information can be used in security Zones 2-5. **Outside entity facilities (including at home)** **Do not** use SECRET information and mobile device that processes, stores or communicates SECRET information for regular ongoing home-based work a. Occasional home-based work is **not recommended**, if required: i. obtain manager approval ii. apply entity procedures on need for a security assessment, and iii. exercise judgement to assess environment risk **Do not** use SECRET information and mobile device that processes, stores or communicates SECRET information anywhere else outside entity facilities (for example private sector offices, café).
Storage	**Do not** leave SECRET information or a mobile device that processes, stores or communicates SECRET information unattended. Store securely when unattended. When storing physical SECRET information: a. inside entity facilities (Zones 3-5 only): i. Zones 4-5, store in Class C container ii. Zone 3, store in Class B container. b. outside entity facilities: **not recommended**, if required for occasional home-based work (see use above): i. apply requirements for carrying outside entity facilities, and ii. retain in personal custody (strongly preferred), or for brief absences from home, store in a Class B or higher container that has been approved as a proper place of custody by the Accountable Authority or their delegate, and iii. return to entity facility as soon as practicable. When storing a mobile device that processes, stores or communicates SECRET information: a. inside entity facilities (Zones 2-5 only): i. Zones 4-5: if in a secured or unsecured state, store in Class C container ii. Zone 3: if in a secured state, Class C container, if unsecured state, store in Class B container iii. Zone 2: if in a secured state, Class B container, if unsecured state, store in a higher zone. b. outside entity facilities **not recommended**, if required for occasional home-based work (see use above): i. apply requirements for carrying outside entity facilities, and ii. retain in personal custody (strongly preferred), or for brief absences from home, exercise judgement to store in a Class C or higher container that has been approved as a proper place of custody by the Accountable Authority or their delegate.

Carry	When carrying physical SECRET information **always retain it in personal custody** a. inside entity facilities: i. Zones 2-5, carry in an opaque envelope or folder that indicates classification ii. Zones 1, carry in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: i. place in a security briefcase, pouch or satchel, and ii. **recommend** tamper-evident packaging if aggregate information increases risk When carrying a mobile device that processes, stores or communicates SECRET information **always retain it in personal custody** a. inside entity facilities: i. Zone 5, if in a secured or unsecured state, apply entity procedures ii. Zones 2-4, carry in secured state; if in an unsecured state, apply entity in procedures iii. Zone 1, carry in a secured state; if in an unsecured state, place inside a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: i. carry in a secured state; if in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper evident seals.
Transfer	When transferring SECRET information: a. inside entity facilities (Zones 1-5): transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if office environment presents very low risk of unauthorised viewing b. to another officer in a different facility: i. apply requirements for carrying outside entity facilities, and ii. transfer by hand, entity safe hand, safe hand courier rated BIL 4, or DFAT courier (if transfer by courier, use tamper evident packaging). Any transfer requires a receipt.
Transmit	When transmitting electronically, communicate over SECRET secure networks (or networks of higher classification). Use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information for any communication that is not over a SECRET network (or network of higher classification).
Official travel	**Travel in Australia** Travelling domestically with SECRET information or with a mobile device that processes, stores or communicates SECRET information is **not recommended**. If required: a. apply requirements for carrying outside entity facilities and any additional entity procedures b. for airline travel, retain as carry-on baggage; if airline requires carry-on baggage to be checked at the gate, i. place in tamper-evident packaging within a security briefcase, pouch or satchel and try to observe entering and exiting the cargo hold and reclaim as soon as possible ii. if tamper-evident packaging not available, **do not travel**. **Do not** leave SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility. **Travel outside Australia** Travelling overseas with SECRET information, or with a mobile device that processes, stores or communicates SECRET information, is **not recommended**—seek DFAT advice on options to access information at destination. If travel with SECRET information or mobile device is required: a. apply requirements for carrying outside entity facilities and any additional entity procedures (entities can consult DFAT for assistance in establishing procedures), consider country-specific travel advice b. for airline travel, retain as carry-on baggage and **do not travel** if the airline requires it to be checked at the gate. If access to SECRET information or mobile device provided at destination: a. apply requirements for carrying outside entity facilities and any additional entity procedures, and b. retain in personal custody or store in an Australian entity facility. **Do not** leave SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility.
Disposal	Dispose of SECRET information using a Class A shredder.

Annex C. Minimum protections and handling requirements for PROTECTED information

BIL 3	PROTECTED—damage to the national interest, organisations or individuals
Protective marking	Apply text-based protective marking **PROTECTED** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For PROTECTED a blue colour is recommended. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. If marking paragraphs, it is recommended that PROTECTED is written in full or abbreviated to (P) and placed either in brackets at the start or end of the paragraph or in the margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle applies to all PROTECTED information. Ongoing access to PROTECTED information requires a Baseline security clearance or above. Any temporary access must be supervised.
Use	PROTECTED information and mobile devices that process, store or communicate PROTECTED information can be used in Zones 1-5. **Outside entity facilities (including at home)** PROTECTED information and mobile devices that process, store or communicate PROTECTED information: a. For regular ongoing home-based work, apply entity procedures, which must include conducting a security risk assessment of the proposed work environment b. For occasional home-based work, apply entity procedures on need for a security assessment and exercise judgement to assess environmental risk c. For anywhere else outside entity facilities (for example private sector offices, café): i. use of physical PROTECTED information is **not recommended**, if required, apply entity procedures and exercise judgement to assess environmental risk ii. use of mobile device that process, store or communicate PROTECTED information: apply entity procedures and exercise judgement to assess environmental risk
Storage	**Do not** leave physical PROTECTED information unattended, store securely when unattended. Mobile devices that process, store or communicate PROTECTED information can be left unattended if in a secured state, subject to entity clear desk policy. When storing physical PROTECTED information: a. inside entity facilities (Zones 2-5 only): i. Zones 4-5, store in lockable container ii. Zones 2-3, store in Class C container b. outside entity facilities: i. for regular ongoing home-based work, install and store in a Class C or higher container ii. occasional home-based work, apply requirements for carrying outside entity facilities, and retain in personal custody (strongly preferred), or for brief absences from home, apply entity procedures and exercise judgement to assess environmental risk. When storing a mobile device that processes, stores or communicates PROTECTED information a. inside entity facilities (Zones 1-5): i. Zones 4-5: if in a secured state, **recommend** storing in lockable container; if in an unsecured state, store in lockable container ii. Zone 2-3: if in a secured state, **recommend** storing in lockable container; if in an unsecured state, store in Class C container iii. Zone 1: if in a secured state, store in Class C container, if unsecured state, store in a higher zone. b. outside entity facilities:

	i. for regular ongoing and occasional home-based work, apply entity procedures and exercise judgement to assess environment risk ii. if in a secured state, **recommend** store in in lockable container; if in an unsecured state, store in a Class C or higher container.
Carry	When carrying physical PROTECTED information **always retain it in personal custody** a. inside entity facilities: i. Zones 1-5, in an opaque envelope or folder that indicates classification b. outside entity facilities (including external meetings) and between entity facilities: i. place in a security briefcase, pouch or satchel, and ii. **recommend** using tamper-evident packaging if aggregate information increases risk. When carrying a mobile device that processes, stores or communicates PROTECTED information a. inside entity facilities: i. Zone 2-5, if in a secured or unsecured state, apply entity procedures ii. Zone 1, carry in secured state; if in an unsecured state, apply entity in procedures b. outside entity facilities (including external meetings) and between entity facilities: i. carry in a secured state; if in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper-evident packaging.
Transfer	When transferring PROTECTED information a. inside entity facilities (Zones 1-5): transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if office environment presents low risk of unauthorised viewing b. to another officer in a different facility i. apply requirements for carrying outside entity facilities, and ii. transfer by hand, entity safe hand, safe hand courier rated BIL 4, or DFAT courier (if transfer by courier, use tamper evident packaging). Any transfer requires a receipt.
Transmit	When transmitting electronically communicate information over PROTECTED networks (or networks of higher classification). Encrypt PROTECTED information for any communication that is not over a PROTECTED network (or network of higher classification).
Official travel	**Travel in Australia** PROTECTED information can be taken to external meetings and on domestic travel. When travelling with PROTECTED information or a mobile device that processes, stores or communicates PROTECTED information: a. apply requirements for carrying outside entity facilities and any additional entity procedures b. for airline travel, retain as carry-on baggage; if airline requires to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim as soon as possible Leaving PROTECTED information, or a mobile device that processes, stores or communicates PROTECTED information, unattended while travelling is **not recommended**. For brief absences from a hotel room, apply entity procedures and exercise judgement to assess environmental risk. **Travel outside Australia** Travelling overseas with physical PROTECTED information is **not recommended**—seek DFAT advice on options to access information at destination. If travel with physical PROTECTED information is required or when travelling a mobile device that processes, stores or communicates PROTECTED information: a. apply requirements for carrying outside entity facilities and any additional entity procedures (entities can consult DFAT for assistance in establishing procedures) and consider country-specific travel advice b. for airline travel, retain as carry-on baggage and **do not travel** if the airline requires it to be checked at the gate. **Do not** leave PROTECTED information or device unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility.
Disposal	Dispose of PROTECTED information using a Class B shredder.

Annex D. Minimum protections and handling requirements for OFFICIAL: Sensitive information

BIL 2	OFFICIAL: Sensitive—limited damage to an individual, organisation or government
Protective marking	Apply text-based protective marking **OFFICIAL: Sensitive** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For OFFICIAL: Sensitive a yellow colour is recommended. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. If marking paragraphs, it is recommended that OFFICIAL: Sensitive is written in full or abbreviated to (O:S) and placed either in brackets at the start or end of the paragraph or in the margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle applies to all OFFICIAL: Sensitive information. There are no security clearance requirements for access to OFFICIAL: Sensitive information.
Use	OFFICIAL: Sensitive information and mobile devices that process, store or communicate OFFICIAL: Sensitive information can be used in Zones 1-5. **Outside entity facilities (including at home)** OFFICIAL: Sensitive information and mobile devices that process, store or communicate OFFICIAL: Sensitive information: a. For regular ongoing and occasional home-based work, apply entity procedures on need for a security assessment, and exercise judgement to assess environmental risk b. For use anywhere else outside entity facilities (for example private sector offices, café), apply entity procedures and exercise judgement to assess environmental risk.
Storage	OFFICIAL: Sensitive information can be left unattended for short periods subject to entity clear desk policy. Mobile devices that process, store or communicate OFFICIAL: Sensitive information can be left unattended if in a secured state. When storing physical OFFICIAL: Sensitive information a. inside entity facilities: i. Zones 1-5, store in lockable container b. outside entity facilities: i. **recommend** placing in an opaque envelope or folder and storing in a lockable container ii. for regular ongoing home-based work, **recommend** store in a Class C or higher container. When storing a mobile device that processes, stores or communicates OFFICIAL: Sensitive information a. inside entity facilities: i. Zones 1-5, if in a secured state, **recommend** storing in lockable container; if in an unsecured state, store in lockable container. b. outside entity facilities: i. for regular ongoing and occasional home-based work, apply entity procedures and exercise judgement to assess environmental risk ii. if in a secured or unsecured state, **recommend** storing in lockable container.
Carry	When carrying physical OFFICIAL: Sensitive information a. inside entity facilities: i. Zones 1-5, **recommend** placing in an opaque envelope or folder b. outside entity facilities (including external meetings) and between entity facilities: i. **recommend** placing in an opaque envelope or folder When carrying a mobile device that processes, stores or communicates OFFICIAL: Sensitive information a. inside entity facilities: i. Zones 1-5, carry in secured state; if in an unsecured state, apply entity in procedures

	b. outside entity facilities (including external meetings) and between entity facilities: i. carry in secured state; if in an unsecured state, apply entity in procedures.
Transfer	When transferring OFFICIAL: Sensitive information a. inside entity facilities (Zones 1-5): i. place in an opaque envelope or folder and apply any additional entity procedures ii. transfer by hand or internal mail. b. to another officer in a different facility i. place in an opaque envelope and apply any additional entity procedures to minimise risk of unauthorised access (eg sealed envelope) ii. transfer by hand, mail or courier; exercise judgement to assess whether registered or other secure mail appropriate.
Transmit	When transmitting electronically communicate information over OFFICIAL networks (or networks of higher classification). Encrypt OFFICIAL: Sensitive information transferred over public network infrastructure, or through unsecured spaces (including Zone 1 security areas), unless the residual security risk of not doing so has been recognised and accepted by the entity.
Official travel	**Travel in Australia** When travelling with OFFICIAL: Sensitive information, or a mobile device that processes, stores or communicates OFFICIAL: Sensitive information, apply requirements for carrying outside entity facilities and any other entity procedures, and exercise judgement to assess environmental risk. If required to leave OFFICIAL: Sensitive information or device unattended while travelling, apply entity procedures and exercise judgement to assess environmental risk. **Travel outside Australia** When travelling overseas with OFFICIAL: Sensitive information or a mobile device that processes, stores or communicates OFFICIAL: Sensitive information apply requirements for carrying outside entity facilities and any additional entity procedures (entities can consult DFAT for assistance in establishing procedures) and consider country-specific travel advice If required to leave OFFICIAL: Sensitive information or device unattended, apply entity procedures and consider country-specific travel advice.
Disposal	Apply entity procedures for disposal.

Annex E. Minimum protections and handling requirements for OFFICIAL information

BIL 1	OFFICIAL—no or insignificant damage
Protective marking	There is no requirement to apply text-based markings to OFFICIAL information. If using text-based markings, apply text-based protective marking **OFFICIAL** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. There is no requirement for colour-based marking for OFFICIAL information. If marking paragraphs, it is recommended OFFICIAL is written in full or abbreviated to (O) and placed either in brackets at the start or end of the paragraph or in margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle is **recommended** for OFFICIAL information. There are no security clearance requirements for access to OFFICIAL information.
Use	OFFICIAL information and mobile devices that process, store or communicate OFFICIAL information, can be used in Zones 1-5 and outside entity facilities.
Storage	OFFICIAL information and mobile devices that process, store or communicate OFFICIAL information can be left unattended, subject to entity clear desk policy. It is **recommended** that mobile devices are in a secured state if left unattended. Apply entity procedures for all storage of OFFICIAL information (ie inside entity facilities and outside entity facilities, including at home. Storage in a lockable container is **recommended** in Zone 1 and outside entity facilities.
Carry	Apply entity procedures when carrying OFFICIAL information.
Transfer	Apply entity procedures for transfer by hand, using internal mail, external mail or courier. For transfers outside entity facilities, it is **recommended** that information be placed in an opaque envelope or folder and sealed to minimise risk of unauthorised access.
Transmit	It is **recommended** that any information communicated over public network infrastructure is encrypted.
Official travel	OFFICIAL information can be taken on domestic and overseas travel. When outside entity facilities, apply entity procedures and consider environmental risk.
Disposal	Apply entity procedures for disposal.

Annex F. Historical classifications and markings

Annex F Table 1 Historical classifications and sensitivity markings

Historical classification or sensitivity marking	Key dates	Current sensitive or classified information level equivalency	Handling
CONFIDENTIAL classification	PSPF recognition of the CONFIDENTIAL classification discontinued on 1 October 2018. The classification is being grandfathered through to October 2020.	None established. Consider the harm and apply corresponding security classification marking	Historical handling protections remain. See Annex F Table 2 and Table 3 for Protection and handling of CONFIDENTIAL information
For Official Use Only (FOUO) dissemination limiting marker (DLM)	FOUO DLM replaced on 1 October 2018. Recognition of the FOUO DLM ceases on 1 October 2020.	FOUO is equivalent to the current OFFICIAL: Sensitive level.	Handling of FOUO information is as per PSPF requirements for OFFICIAL: Sensitive information.
Sensitive DLM	Sensitive DLM replaced on 1 October 2018. Recognition of the Sensitive DLM ceases on 1 October 2020.	Unless otherwise classified, Sensitive is equivalent to the current OFFICIAL: Sensitive level. The (optional) *Legislative secrecy* information management marker may be applied.	Handling of Sensitive information is: a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL: Sensitive information.
Sensitive: Cabinet DLM	Sensitive: Cabinet DLM replaced on 1 October 2018. Recognition of the Sensitive: Cabinet DLM ceases on 1 October 2020.	The Sensitive: Cabinet DLM is equivalent to the current CABINET caveat.	Handling of Sensitive: Cabinet information is as per: a. the identified classification level and b. PSPF (and supporting Security Caveats Guidelines) requirements for the CABINET caveat.
Sensitive: Legal DLM	Sensitive: Legal DLM replaced on 1 October 2018. Recognition of the Sensitive: Legal DLM ceases on 1 October 2020.	Unless otherwise classified, Sensitive: Legal is equivalent to the current OFFICIAL: Sensitive level. The (optional) *Legal privilege* information management marker may be applied.	Handling of Sensitive: Legal information is: a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL: Sensitive information.
Sensitive: Personal DLM	Sensitive: Personal DLM replaced on 1 October 2018. Recognition of the Sensitive: Personal DLM ceases on 1 October 2020.	Unless otherwise classified, Sensitive: Personal is equivalent to the current OFFICIAL: Sensitive level. The (optional) *Personal privacy* information management marker may be applied.	Handling of Sensitive: Personal information is: a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL: Sensitive information.
HIGHLY PROTECTED classification	Recognition of the HIGHLY PROTECTED classification ceased on 1 August 2012.	HIGHLY PROTECTED is equivalent to the current SECRET classification.	Handling of HIGHLY PROTECTED information is as per PSPF requirements for SECRET information.
RESTRICTED classification	Recognition of the RESTRICTED classification ceased on 1 August 2012.	RESTRICTED is equivalent to the current OFFICIAL: Sensitive level.	Handling of RESTRICTED information is as per PSPF requirements for OFFICIAL: Sensitive information.
X-IN-CONFIDENCE classification	Recognition of the X-IN-CONFIDENCE classification ceased on 1 August 2012.	X-IN-CONFIDENCE is equivalent to the current OFFICIAL: Sensitive level.	Handling of X-IN-CONFIDENCE information is as per PSPF requirements for OFFICIAL: Sensitive information.

Protection and handling of CONFIDENTIAL information

The historical classification CONFIDENTIAL does not have an equivalent level of classification under the current PSPF. Information that was classified as CONFIDENTIAL before October 2020 has a business impact level of very high. This means that the compromise of CONFIDENTIAL information's confidentiality would be expected to cause significant damage to the national interest, organisations or individuals. **Annex F Table 2** provides the sub-impact categories for this business impact level.

Annex F Table 2 Business Impact Level of CONFIDENTIAL information: Business Impact Level 3A

Sub-impact categories	Significant damage is:
Impacts on national security	causing damage to national security.
Impacts on entity operations	a. causing a severe degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform one or more of its functions for an extended time b. resulting in major long-term harm to entity assets.
Australian financial and economic impacts	a. undermining the financial viability of, or causing substantial financial damage to, a number of major Australia-based or Australian-owned organisations or companies b. causing long-term damage to the Australian economy to an estimated total of $10 to $20 billion c. causing major, short-term damage to global trade or commerce, leading to short-term recession or hyperinflation in Australia.
Impacts on government policies	a. significantly disadvantaging Australia in international negotiations or strategy b. temporarily damaging the internal stability of Australia or friendly countries c. causing significant damage or disruption to diplomatic relations, including resulting in formal protest or retaliatory action.
Impacts on personal safety	endangering small groups of individuals – the compromise of information could lead to serious harm or potentially life threatening injuries to a small group of individuals
Impacts on crime prevention	causing major, long-term impairment to the ability to investigate serious offences, ie offences resulting in two or more years imprisonment.
Impacts on defence operations	causing damage to the operational effectiveness or security of Australian or allied forces that could result in risk to life.
Impacts on intelligence operations	causing damage to Australian or allied intelligence capability.
Impacts on national infrastructure	damaging or disrupting significant national infrastructure.

The following information describes the minimum protections and handling for legacy CONFIDENTIAL information.

Annex F Table 3 Minimum protection and handling for CONFIDENTIAL information

BIL 3.5	CONFIDENTIAL—significant damage to the national interest, organisations or individuals
Protective marking	Maintain text-based protective marking **CONFIDENTIAL** to documents (including emails). If text-based markings were not used, maintain colour-based markings. For CONFIDENTIAL a green colour was used historically. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. From October 2020, do not mark new information as CONFIDENTIAL. For new information that would previously have been marked CONFIDENTIAL, consider the harm and apply corresponding security classification marking under the current PSPF.
Access	The need-to-know principle applies to all CONFIDENTIAL information. Ongoing access to CONFIDENTIAL information requires a Negative Vetting 1 security clearance or above. Any temporary access must be supervised.
Use	CONFIDENTIAL information and mobile devices that process, store or communicate CONFIDENTIAL information can be used in security Zones 1-5. **Outside entity facilities (including at home)** CONFIDENTIAL information and mobile device that processes, stores or communicates CONFIDENTIAL information: a. **do not** use for regular ongoing home-based work

	a. occasional home-based work **not recommended**, but if required, obtain manager approval, apply entity procedures on need for a security assessment, and exercise judgement to assess environment risk b. **do not** use elsewhere (for example café).
Storage	**Do not** leave CONFIDENTIAL information or a mobile device that processes, stores or communicates CONFIDENTIAL information unattended, store securely when unattended. When storing physical SECRET information a. inside entity facilities (Zones 2-5 only): i. Zones 3-5, store in Class C container ii. Zone 2, store in Class B container. b. Outside entity facilities **not recommended**, if required for occasional home-based work (see use above): i. apply requirements for carrying outside entity facilities, and i. retain in personal custody (strongly preferred), or for brief absences from home, store in Class B or higher container (container must be approved as a proper place of custody by the Accountable Authority or their delegate), and return to entity facility as soon as practicable. When storing a mobile device that processes, stores or communicates CONFIDENTIAL information a. inside entity facilities (Zones 2-5 only): i. Zones 3-5: if in a secured or unsecured state, store in Class C container i. Zone 2: if in a secured state, Class B container, if unsecured state, store in a higher zone. b. Outside entity facilities **not recommended**, if required for occasional home-based work (see use above): i. apply requirements for carrying outside entity facilities, and ii. retain in personal custody (strongly preferred), or for brief absences from home, exercise judgement to store in a Class C container.
Carry	When carrying physical CONFIDENTIAL information a. inside entity facilities: i. Zones 2-5, retain in personal custody in an opaque envelope or folder that indicates Classification ii. Zones 1, retain in personal custody in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: i. retain in personal custody ii. place in a security briefcase, pouch or satchel, and iii. **recommend** tamper-evident packaging if aggregate information increases risk. When carrying a mobile device that processes, stores or communicates CONFIDENTIAL information a. inside entity facilities: i. Zone 5, if in a secured or unsecured state, apply entity procedures i. Zones 2-4, carry in secured state; if in an unsecured state, apply entity in procedures ii. Zone 1, carry in a secured state; if in an unsecured state, place inside a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: i. in a secured state, retain in personal custody ii. in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper evident seals.
Transfer	When transferring CONFIDENTIAL information a. inside entity facilities (Zones 1-5): transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if office environment presents very low risk of unauthorised viewing b. to another officer in a different facility i. apply requirements for carrying outside entity facilities, and ii. transfer by hand, entity safe hand, safe hand courier rated BIL 4, or DFAT courier (if transfer by courier, use tamper evident packaging). Any transfer requires a receipt.

Transmit	When transmitting electronically communicate over SECRET secure networks (or networks of higher classification). Use ASD's High Assurance Cryptographic Equipment to encrypt CONFIDENTIAL information for any communication that is not over a SECRET network (or network of higher classification).
Official travel	**Travel in Australia** When travelling with physical CONFIDENTIAL information: a. apply requirements for carrying outside entity facilities and any additional entity procedures a. for airline travel, retain as carry-on baggage and if airline requires to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim ASAP b. **do not** leave CONFIDENTIAL information unattended, retain in personal custody, and c. **do not** store while travelling (eg in a hotel room), if storage required, store in an Australian entity facility. When travelling with a mobile device that processes, stores or communicates CONFIDENTIAL information: a. apply requirements for carrying outside entity facilities and any additional entity procedures b. **not recommended** for airline travel, if required, retain as carry-on baggage and if airline requires to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim ASAP c. **do not** leave CONFIDENTIAL information unattended, retain in personal custody, and d. **do not** store while travelling, if storage required, store in an Australian entity facility. **Travel outside Australia** **Not recommended** to travel overseas with physical CONFIDENTIAL information. If required, follow entity procedures, and if required, consult DFAT. **Do not** travel overseas with a mobile device that processes, stores or communicates CONFIDENTIAL information. If required, see DFAT advice on options to access information at destination.
Disposal	Dispose of CONFIDENTIAL information using a Class A shredder or entity-assessed and approved or NAID AAA certified destruction service with specific endorsement and approved equipment and systems.

Annex G. Email protective marking standard

The Email protective marking standard provides guidance for applying protective markings (and, where relevant, information management markers) on emails exchanged in and between Australian Government entities.

Access the standard here - (add link to PDF and Word versions of EPMPS)

Annex H. Sample case studies

The following case studies are examples that entities may wish to draw on or adapt in establishing their procedures and operational controls. These are examples of application of the policy only, and the Attorney-General's Department recommends that entities consider whether the examples provided meet entity-specific requirements and are suitable for use in conjunction with existing entity procedures.

Entity personnel should not rely on these examples for advice on how to apply the PSPF—consult a security advisor in your entity to ensure you are applying the PSPF in accordance with your entity's security plan and procedures.

Case study: Example of information declassification for increased sharing

The Productivity Commission Data Availability and Use report indicates that a wide range of government data can be shared. The availability and usefulness of data delivers benefits to the community, engenders community trust and confidence in how data is managed and used and preserves commercial incentives to collect, maintain and add value to data.

For example, there is potential for data about health service provider costs and performance, as well as de-identified linked data about health service recipients, that can be used for effective and targeted service interventions and improved health outcomes.

Identifying characteristics that appear predictive during data analysis can provide valuable insights into the effectiveness of various policies and interventions, allowing new services to emerge in response to community demand.

By de-identifying the health service recipients' data or redacting sensitive personal details, the information is no longer considered to be OFFICIAL: Sensitive (as it does not include sensitive information under the Privacy Act or other measures of harm) and can be shared. If desirable, the protection markings for OFFICIAL can be applied to the information.

Case study: Using TOP SECRET information in a Zone 3

An officer with NV2 clearance wants to read a TOP SECRET document in a Zone 3 within the entity. In accordance with the minimum protections outlined in **Annexure A**, the officer assesses their surroundings to judge whether the people and equipment within their proximity are likely to compromise the officer's ability to protect the information from unauthorised access.

The officer notes that several of the people around them are contractors without security clearances. The officer judges that there is a high probability that an unauthorised person may see the material and decides the information could be more easily secured from unauthorised viewing by moving to a nearby meeting room within the Zone 3 to read the material. Before moving to the meeting room, the officer puts the material in a folder with TOP SECRET indicated on the front.

Case study: Physical presence when at home in Australia

An officer is attending an early morning meeting tomorrow in another government building in the same city in Australia. The officer requires access to a PROTECTED document for use at the meeting. Given the meeting starts at 6:30am close to where the officer lives, the officer's manager has given approval for them to take the material home overnight providing the officer:

(i) confirms the external meeting will take place in a meeting room that is a security zone

(ii) secures the information from unauthorised access by using double-enveloping (in a sealed envelope inside a security briefcase)

(iii) does not open or use the information until the officer is in the secure meeting room, and

(iv) keeps the information in their personal custody/physical presence (ie keeps the secured information in the same room with them, including while asleep).

While the officer is at home, they remember a dinner engagement at the local restaurant. The officer judges that taking the security briefcase with them would draw attention and determines the information would be safer left at home. The officer stores the security briefcase in a lockable cabinet and heads to dinner. As soon as the officer returns home, they retrieve the briefcase, open it to confirm the information is still sealed within, and then keep the briefcase with them until returning to their entity's facility after the meeting.

Case study: Removing TOP SECRET information from entity facilities to use in a meeting

An officer with a NV2 security clearance needs to remove a TOP SECRET document from the entity facility to attend an external meeting.

The officer knows that this practice is not recommended but the meeting organisers have advised they are unable to make the material available to attendees and requested they bring a copy with them. The officer takes the following steps to ensure the protection of the information:

(i) confirms the external meeting will take place in a government meeting room that is at lease a Zone 3

(ii) seeks their manager's written approval to remove the material, and keeps a record of the approval

(iii) records the information is being removed with manager approval in the team's Classified Document Register

(iv) secures the information from unauthorised access by enclosing the TOP SECRET information in a tamper evident envelope, and placing it in a security satchel

(v) ensures the material remains unopened until the officer is in the Zone 3 meeting room.

When the meeting concludes, the officer secures the TOP SECRET information in a tamper evident envelope and places it in the security satchel, where it remains unopened until the officer is back in a Zone 3 or higher of the entity facility.

Once back in the office, the officer updates the Classified Document Register to confirm the material has been returned to the entity facility.