Changes in revised PSPF Policy 8: Sensitive and classified information

Location of change	Description of change	Rationale
A. Purpose	Purpose amended to reflect a security classification is applied to protect the confidentiality of information or assets holding information.	This addition provides clarity to one of the purposes of the policy—providing guidance so entities correctly classify their information—by making clear the link between security classifications and confidentiality risks, and minimises misunderstanding that security classifications are designed only to protect integrity and availability of information.
B.1 Core requirement	References to 'information asset holdings' have been amended to 'information holdings'.	The use of the term 'information asset holdings' is not used elsewhere in the policy. Additionally, the term itself could be confusing as the PSPF generally differentiates between three types of resources: people, information and assets.
B.2 Supporting requirements	Text changes to opening of section.	These changes better reflect that some supporting requirements apply to entities that are not the originator of the information.
B.2 Supporting requirements *Requirement 1*	Minor text changes: a. Title of requirement has changed from 'Identifying information assets' to 'Identifying information holdings'. b. The requirement now refers to 'official information', rather than just referring to an official record.	These changes ensure clarity and consistency of text across the policy: a. ensures consistency with B.1 Core requirement. b. creates a clearer link to the explanation of 'official information' at C.1 Official information.
B.2 Supporting requirements *Requirement 2*	The description of the compromise of UNOFFICIAL and OFFICIAL information confidentiality has changed from 'not applicable': a. for UNOFFICIAL, to 'no damage'. b. for OFFICIAL, to 'no or insignificant damage'.	These changes were requested by stakeholders clarify how the Business Impact Levels (BILs) apply to UNOFFICIAL and OFFICIAL information.
B.2 Supporting requirements *Requirement 3*	This requirement (declassification) has moved from Requirement 4 to Requirement 3. Content unchanged.	Change to reflect flow of guidance.
B.2 Supporting requirements *Requirement 4(c)*	Removed previous text for Requirement 4(c) and replaced with: *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.*	The previous text for Requirement 4(c) mandated that entities have a protective marking scheme to deal with scenarios such as verbal discussions, but did not mandate that entities apply their scheme (although training of staff in the scheme was mandated).
B.2 Supporting requirements *Requirement 5*	This requirement (Using metadata to mark information) has moved from PSPF Policy 9 to PSPF Policy 8.	This requirement was previously in PSPF Policy 9: Access to information. There is **no change** to the scope of the requirement.

Location of change	Description of change	Rationale
		Stakeholders indicated this requirement was more relevant in the context of requirements in PSPF Policy 8.
B.2 Supporting requirements *Requirement 6*	Additional requirement added at 6(c): *For all caveated information, entities **must** apply the protections and handling requirements established by caveat owners in the Australian Government Security Caveats Guidelines.*	Change to ensure that in addition to the protections outlined in Annexes A-D, the minimum protections for caveated information (outlined in the Security Caveat Guidelines) are also mandated.
B.2 Supporting requirements *Requirements 7-9*	These requirements now include references to Annexes A-D that mandate the minimum protections for the handling, storage and disposal of information. Entities will be expected to meet the minimum protections in these annexures.	Feedback from stakeholders indicated a need for clearer guidance, including practical real-life examples, to assist entities in meeting the policy requirements.
C.1 Official information	Table 1, which outlined scenarios of 'information compromise', has been removed. The explanation of information compromise has been embedded in the policy text.	
C.2 Sensitive and security classified information	Text has been added to: a. reiterate that the originator determines classification of information, as per Requirement 1 of Policy 8. b. explain when an asset should be treated as a classified asset (ie the guidance to assess the BIL of information also applies when assessing the BIL of assets holding information, such as laptops).	These changes: a. make clear that the policy obligations rest on the entity (although the obligations are given effect through the actions of officers). b. support the 'classified assets' in *PSPF Policy 15 Physical security for entity resources*, by making clear entities should apply the Business Impact Levels to the information held on an asset to determine whether security classification protections should also be applied to the asset.
C.2.1 Proper use of security classifications	This is a new section, using existing text from the previous Policy 8 ('When to assess information sensitivity or security classification' and 'Assessing whether information is sensitive or security classified').	Bringing this information together clarifies and strengthens the narrative rationale for the proper use of security classifications
C.2.2 Who assess information sensitivity or security classification	The text defining 'originator' has been removed.	Originator has already been defined within the policy, at B.2 Supporting requirements.
C.2.4 How to assess information sensitivity or security classification	Changes are to: a. recast the text discussing using the BIL tool to assess the impact of compromise of information's availability or integrity. b. move the footnoted examples of OFFICIAL: Sensitive information to a	These changes: a. make clearer the existing position in Policy 8 that having a high BIL for integrity or availability compromise does not mean information should be security classified, although may mean security measures are warranted. b. feedback from stakeholders indicated a

Location of change	Description of change	Rationale
	table in the body of the document.	need for clearer guidance, including for practical real-life examples be provided throughout the policy.
C.2.4 How to assess information sensitivity or security classification *Table 1 Business Impact Levels tool*	This table has been updated to: a. describe the BILs for UNOFFICIAL and OFFICIAL information as 'no damage' and 'no or insignificant damage' respectively. b. make clear that for OFFICIAL: Sensitive a business level impact assessment needs to consider potential impact on government and not potential impact to the national interest.	The changes: a. ensure consistency with new Requirement 2 (see B.2 Supporting requirements). b. clarify how policy is intended to operate; no substantive change to policy.
Figure 1 Assessing whether information is sensitive or security classified	This figure has been reformatted, and the detail about information management markers removed.	The changes make the figure easier to read and print on an A4 page for reference. The details on information management markers (IMMs) were removed as including this in the figure has the potential to confuse the reader; unlike protective markings, applying IMMs to information is optional.
C.2.5 Sanitising, reclassifying or declassifying information	Changes: a. amend the text on automatically declassifying information. b. add a recommendation that entities have procedures to reclassify or declassify information and give examples of the situations where the procedures could apply.	These changes: a. clarify the trigger points for when entities should automatically declassify information b. address feedback from stakeholders indicating a need for clearer guidance, including for practical real-life examples to be provided throughout Policy 8.
C.2.6 Historical security classifications	New content to provide guidance on historical security classifications and other protective markings.	Improved link to guidance in Annex F.
Tables 3, 4 and 5 (original)	Content removed from Tables 3–5 and incorporated into Annexes A-D. • Table 1 Minimum protective markings for sensitive and security classified information • Table 2 Disclosure or access (for more information, see core requirement on access to information) • Table 3 Audits and registers	These changes were to provide a consolidated list of minimum protections for each level of sensitive and security classified information (Annexes A-D).
C.4 Information management markers	This new section outlines when and which information management markers could be applied to information.	Stakeholders indicated they expect to find this requirement and guidance in Policy 8. Including this section provides greater clarity within the policy when considering the section on protective markings, which refer to information management markers. It also supports new Requirement 5 (Using metadata to mark information).

Location of change	Description of change	Rationale
C.5.1.1 Applying text-based protective markings	A recommended approach to using paragraph grading indicators has been added, although these will continue to be optional under the policy.	Providing a recommended approach will help promote a consistency across those agencies who utilise paragraph grading indicators.
C.5.1.2 Applying protective markings if text-based markings cannot be used	More detail has been provided around the use of colour-based markings, including a recommendation that Yellow be used for OFFICIAL: Sensitive information.	Stakeholders have indicated a desire for a colour-based marking for OFFICIAL: Sensitive. While Green was suggested, this could pose issues for agencies with active CONFIDENTIAL files, a classification previously assigned Green.
C.5.1.3 Using metadata to apply protective markings	This is a new section providing guidance on new Requirement 5 (Using metadata to mark information).	Stakeholders indicated they expect to find this requirement (and hence guidance to meet it) in Policy 8.
C.5.3 Using sensitive and security classified information	This is a new section emphasising the importance of considering the physical environment when using sensitive and security classified information.	Addresses the gap within the PSPF on protecting information in verbal communications, which was previously not specifically addressed (in Policy 8 or in the related *PSPF Policy 15 Physical security for entity resources*).
C.5.3.1 Using information when working away from the office	This is a new section providing guidance for using sensitive and security classified information outside entity facilities, including for home-based work.	The previous policy did not address use of sensitive and security classified information outside entity facilities, despite this being a practice of some officers. Annexes A-D that support Requirements 7-9 indicate whether use outside of entity facilities is permitted for each level of sensitive and security classified information, and the minimum protections in such scenarios.
C.5.3.2 Using information on mobile computer and communications	This is a new section providing guidance for using information on mobile devices.	The previous policy did not provide sufficient information on using mobile devices. Annexes A-D establish the minimum protections for accessing, storing or communicating sensitive and security classified information on mobile devices.
C.5.3.3 Using information on official travel outside Australia	This is a new section to provide clearer guidance in support of the minimum protections outlined in Annexes A-D.	
C.5.4 Storing sensitive and security classified information	New text has been added to make clear that information is deemed to be 'in storage' when it is unattended.	This change makes clear at what point the requirements around storage of information are triggered.
C.5.4.1 Clear desk, session and screen locking procedures	This is a new section providing recommendations about what clear desk, session and screen locking procedures should encompass, including their purpose.	The previous policy indicated these procedures should be in place, but did not detail what such procedures should entail.
C.5.5 Carrying sensitive and security classified information	This is a new section providing guidance on carrying sensitive and classified information from one location to another.	To address the confusion around the different between transferring information (from one person or place to another) and

Location of change	Description of change	Rationale
		carrying information, particularly in less secure zones or public spaces.
C.5.6 Transferring physical sensitive and security classified information	Examples of typical real-life transfer situations have been added.	Feedback from stakeholders indicated a need for clearer guidance, including for practical real-life examples be provided throughout the policy.
C.5.6.1 Preparing information for transfer	The text outlining the recommended approach to physically transfer physical sensitive and security classified information has been amended, to recommend a 'layering approach', and provide detailed, real-life examples of how to achieve this.	Combined with the new annexures to support Requirements 7-9, these changes provide more specific, clearer guidance to secure information for transfer, responding to the feedback from stakeholders indicating a need for clearer guidance, including for practical real-life examples. Annexes A-D establish the minimum protections (ie the number of layers) required for the transfer of each level of sensitive and security information.
C.5.6.3 Transferring information outside Australia	This is a new section explaining the process for transferring security classified information overseas.	The previous policy did not provide guidance for transferring security classified information overseas. Annexes A-D establish the minimum protections for transferring sensitive and security classified information overseas.
C.5.6.4 Electronically transmitting sensitive and security classified information	This is a new section explaining that Requirement 7 (Transfer) covers electronic transfer and transmission of sensitive and security classified information. It includes a table setting out the minimum protections for transmitting sensitive and security information electronically.	The previous policy did not provide guidance for transferring sensitive and security classified information via electronic means. Including this guidance clarifies that Requirement 7 (Transfer) also applies to transfer via electronic means and provides support for entities to meet Requirement 7 (Transfer).
C.5.7 Disposing of sensitive and security classified information	Principle 6 of the National Archives of Australia Information Management Standard has been extracted and added to this section.	This provides additional context for the guidance on disposing of sensitive and security classified information.
C.5.7.1 Destroying sensitive and security classified information	Text has been added to this section to explicitly state that Requirement 9 does not apply to OFFICIAL information, alongside a recommendation that entities put in place procedures to securely destroy OFFICIAL and OFFICIAL: Sensitive information.	

List of new Annexes

Annex Ref	Content
Annex A	Consolidated content to provide minimum protections and handling requirements for TOP SECRET information
Annex B	Consolidated content to provide minimum protections and handling requirements for SECRET information

Annex C	Consolidated content to provide minimum protections and handling requirements for PROTECTED information
Annex D	Consolidated content to provide minimum protections and handling requirements for OFFICIAL: Sensitive information
Annex E	Consolidated content to provide minimum protections and handling requirements for OFFICIAL information
Annex F	Historical classifications and markings
Annex G	Email protective marking standard
Annex H	Sample case studies