Australian Government
Attorney-General's Department

Protective Security Policy Framework

Security Classification Reforms

All official information requires an appropriate degree of protection—any deliberate or accidental compromise[1] of information could adversely affect government business. The PSPF defines the Australian Government's security classifications and associated handling protections.

How to handle sensitive and security classified information

Key operational controls to protect sensitive and security classified information include:

a. identifying sensitive and security classified information
    i. with a protective marking
    ii. by creating an auditable record of all incoming and outgoing material, transfer, copy or movements for, at a minimum, TOP SECRET information and other accountable material
b. limiting disclosure or access to sensitive and security classified information to personnel with:
    i. a demonstrated need-to-know the content of the information
    ii. an applicable security clearance
c. transferring and transmitting information by means which deter and detect unauthorised access
d. storing and using information securely
e. destroying and disposing of information by secure means.

A. What has changed?

The reforms simplify the existing classification system as follows:

Then	→	Now
TOP SECRET	**Security classifications**	TOP SECRET
SECRET		SECRET
CONFIDENTIAL		N/A (discontinued)
PROTECTED		PROTECTED
Sensitive: Cabinet	**DLM→Caveat**	CABINET (Caveats[2], other than NATIONAL CABINET[3], can only be applied with security classified information)
Sensitive	**DLM→Information management marker**	Apply classification or OFFICIAL: Sensitive and optional information management markers: • Legislative secrecy • Personal privacy • Legal privilege
Sensitive: Personal		
Sensitive: Legal		
For Official Use Only	**DLM→DLM**	OFFICIAL: Sensitive
UNCLASSIFIED	**Non-classification markings**	OFFICIAL
UNOFFICIAL		UNOFFICIAL

These changes are reflected in the new Email protective marking standard at Annex G of the PSPF policy 8: Sensitive and classified information.

---

[1] Information compromise includes, but is not limited to: loss, misuse, interference, unauthorised access, unauthorised modification and unauthorised disclosure.
[2] Refer to the the Australian Government Security Caveat Guidelines for special handling and use instructions for caveats.
[3] The NATIONAL CABINET caveat commences on 1 December 2020, with implementation by all NCCEs who are required to use this caveat, required by 31 March 2021.

B. Assessing sensitive or security classified information[4]

In order to determine what protective marking to use, the originator (author/creator of the information) assesses its sensitivity or security classification by considering the potential impacts to national interest, organisations or individuals that could arise from compromise of the information's confidentiality.

Was the information created, sent or received as part of your work for the government?

YES **This is official information and may need a protective marking or security classification**

NO

Would compromise of the information's confidentiality cause <u>exceptionally grave damage</u> to the national interest, organisations or individuals?
For example, but not limited to, directly provoking international conflict or causing exceptionally grave damage to relations with friendly governments.

YES **This information needs the highest degree of protection.**
It is security classified TOP SECRET

NO

Would compromise of the information's confidentiality cause <u>serious damage</u> to the national interest, organisations or individuals?
For example, but not limited to, information that, if compromised, could shut down (or substantially disrupt) significant national infrastructure.

YES **This information needs a substantial degree of protection.**
It is security classified SECRET

NO

Would compromise of the information's confidentiality cause <u>damage</u> to the national interest, organisations or individuals?
For example, but not limited to, information that, if disclosed without authorisation or otherwise compromised, could reasonable be expected to:

- cause a severe degradation in (or loss of) organisational capability to an extent and duration that entity cannot perform one or more of its primary functions
- seriously impeded development or operation of major policies.

YES **This information needs a moderate degree of protection.**
It is security classified PROTECTED

NO

Is it caveated information not already captured by a higher security classification?
For example, but not limited to, CABINET information

YES **This information needs a security classification of at least PROTECTED**
(except the NATIONAL CABINET caveat which can be applied with OFFICIAL: Sensitive information or above)

NO

Would compromise of the information's confidentiality cause <u>limited damage</u> to the national interest, organisations or individuals?

YES **This information is OFFICIAL: Sensitive**
This information does not need a security classification. It needs protection and limitation of access to those with a need-to-know.

NO

This is OFFICIAL information
This is the majority of official information that is created or processed by the public sector.
Marking information as OFFICIAL is optional, but may be required by ICT systems (eg email).

This is UNOFFICIAL information
Marking information as UNOFFICIAL is optional, but may be required by ICT systems (eg email).

Three terms from the 'Rights' property of the AGRkMS have been designated as information management markers: Legal privilege, legislative secrecy and personal privacy. They are recommended to be applied with OFFICIAL: Sensitive information and above. While categorising information content by non-security access restrictions is not mandated in the PSPF, the Rights Type Scheme provides a standard set of terms ensuring common understanding, consistency and interoperability across systems and government entities. For guidance, see the PSPF policy 8: Sensitive and classified information.

[4] There are historical security classifications and other protective markings 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 Historical markings table.

Transition timeframes and milestones

There is an extended transition period for these reforms, full implementation is required by 1 October 2020. Entities **must not** send and receive emails from non-corporate Commonwealth entities (NCCE)[5] using the old classification system after 1 October 2020.

Arrangements for receiving emails from other sources

Arrangements for receiving emails from sources that are not required to adhere to the PSPF remain the same (eg emails from state and territory entities, corporate Commonwealth entities, Commonwealth companies and non-government organisations). Gateways will need to accommodate incoming emails from these sources bearing different markings.

	1 October 2018	1 January 2019	1 October 2020
Implementation stage	**PSPF REFORMS 2018 COMMENCES** Transition to new system commences.	**NEW CLASSIFICATION SYSTEM[6] STARTS** Collective government *start date* to accept and receive emails under the new system. All entities **must** ensure that their systems will not block emails that are marked under either the new or old system.	**OLD CLASSIFICATION SYSTEM[7] CEASES** Entities **must not** send or receive emails from NCCEs under the old system after this date.[8]
	Entities commence preparations to implement the new system in accordance with PSPF Policy: [Sensitive and classified information](#). Entities prepare their email systems to accept messages according to the new scheme and update supporting internal ICT systems. This includes establishing entity procedures, engaging with service providers and educating personnel on the new system.	During January 2019 to September 2020, entities: • continue to educate personnel/users on new arrangements • shift to marking new documents with new PSPF arrangements • grandfather current holdings of classified and DLM material—noting that existing holdings do not need to be reclassified (historical handling protections remain).	After 1 October 2020, entities **must** use the new classification system for both internal and external communication. Entities **must not** send to or receive emails from NCCEs using markings under the old system after this date. Arrangements for receiving emails from sources other than NCCEs remain the same.[8]
Internal NCCE communication	**Send:** old **or** new system **Receive:** old **or** new system	**Send:** old **or** new system **Receive:** old **or** new system	**Send: only** new system **Receive: only** new system
External NCCE communication	**Send : *only*** old system (***must not*** send externally under new system) **Receive: *must*** accept old system	**Send:** old **or** new system **Receive: *must*** receive old and new system	**Send: only** new system **Receive:** new system[8]

[5] As defined under the PGPA Act. Refer to the PGPA Act Flipchart of Commonwealth entities and companies.
[6] Old classification system is the Australian Government Security classification System (PSPF 2014)
[7] New classification system is PSPF policy: Sensitive and classified information (PSPF 2018)
[8] Entity arrangements for receiving emails from sources other than NCCEs remain the same (eg emails from state and territory entities, corporate Commonwealth entities, and non-government organisations).

Markings ceasing on 1 October 2020

For DLMs and classification markings due to cease on 1 October 2020, entities are strongly encouraged not to create new material using these markings after 1 January 2019. These markings must not be used after 1 October 2020.

Marking	Key dates	Replacement equivalency	Handling
CONFIDENTIAL classification	CONFIDENTIAL classification is discontinued from 1 October 2018. Recognition of the CONFIDENTIAL classification ceases on 1 October 2020.	None established. Consider the harm and apply corresponding security classification marking.	Historical handling protections remain.
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.
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.
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 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.
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.

Historical markings (ceased 1 August 2012)

Historical marking	Key dates	Current equivalency	Handling
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.
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.
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.