NSW GOVERNMENT | Customer Service

Review of Information Classification, Labelling and Handling Guidelines

Records Managers' Forum

27 November 2019

www.customerservice.nsw.gov.au

Information classification, labelling and handling

Information compromise

- Loss
- Misuse
- Interference
- Unauthorised access
- Unauthorised modification
- Unauthorised disclosure

NSW Cyber security policy

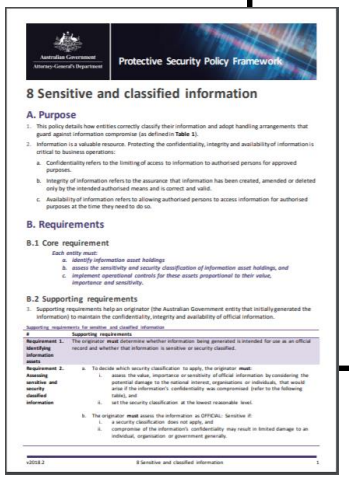
3.3 **Classify information** and systems according to their importance (i.e. the impact of loss of confidentiality, integrity or availability), and

- assign ownership
- **implement controls according to their classification** and relevant laws and regulations
- Identify the Agency's "crown jewels" and report them to Cyber Security NSW as per mandatory requirement 5.3.

Why Review? Change to the Australian Government System

Australian Government
Attorney-General's Department

The Protective Security Policy Framework


Protective Security Policy Framework

8 Sensitive and classified information

A. Purpose

B. Requirements

B.1 Core requirement

B.2 Supporting requirements

NSW GOVERNMENT

NSW Government Information Classification, Labelling and Handling Guidelines


Finance, Services & Innovation

Please note, this document is under review (2019).

NSW Government Information Classification, Labelling and Handling Guidelines

July 2015

Department of Finance, Services and Innovation
Level 23, McKell Building
2-24 Rawson Place
SYDNEY NSW 2000

August 2015

https://www.protectivesecurity.gov.au/sites/default/files/2019-11/pspf-infosec-08-sensitive-classified-information.pdf

Changes to Sensitive and security classified information

8 Sensitive and security classified information

What are the changes? Dissemination Limiting Markers (DLMs)

From	To	
DLM	**DLM**	**IMM** (Optional)
For Official Use Only	OFFICIAL: Sensitive	Legal Privilege
Sensitive		Legislative secrecy
Sensitive: Personal		Personal privacy
Sensitive: Legal		
Sensitive: Cabinet*		

* Caveat

NSW – Dissemination Limiting Markers

From	To
DLM	**DLM**
For Official Use Only	OFFICIAL: Sensitive
Sensitive	OFFICIAL: Sensitive
Sensitive: Personal	OFFICIAL: Sensitive – Personal
Sensitive: Legal	OFFICIAL: Sensitive – Legal
Sensitive: Cabinet	No longer a DLM, now a caveat
Sensitive: NSW Government	OFFICIAL: Sensitive – NSW Government
Sensitive: NSW Cabinet	OFFICIAL: Sensitive – NSW Cabinet
Sensitive: Law Enforcement	OFFICIAL: Sensitive – Law Enforcement
Sensitive: Health Information	OFFICIAL: Sensitive – Health Information

Other changes – Security classifications

From	To
Security Classification	**Security Classification**
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	Removed*
PROTECTED	PROTECTED

*Consider the harm and apply corresponding security classification marking

Other changes – Other markings

From	To
Other marking (Optional)	**Other marking** (Optional)
UNCLASSIFIED	OFFICIAL
UNOFFICIAL*	UNOFFICIAL

*Not currently used in NSW

Overview – proposed application of changes in NSW

Security Classification

TOP SECRET
SECRET
PROTECTED

Caveat

Cabinet

DLM

OFFICIAL: Sensitive
OFFICIAL: Sensitive – Personal
OFFICIAL: Sensitive – Legal
OFFICIAL: Sensitive – NSW Government
OFFICIAL: Sensitive – NSW Cabinet
OFFICIAL: Sensitive – Law Enforcement
OFFICIAL: Sensitive – Health Information

Other markings

(Optional)

OFFICIAL
UNOFFICIAL

Assessing information sensitivity or security classification

- The Business Impact Levels are aligned with the protective markings, making them easier to apply.

Now

Table 2 Business Impact Levels tool – Assessing damage to the national interest, organisations or individuals

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 that is created or processed by the public sector. This includes routine business operations and services.	While not a security classification, OFFICIAL: Sensitive information is that which would result in **limited damage** to an individual, organisation or government if compromised.	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.

Before

1 (Low-medium)	2 (High)	3 (Very High)	4 (Extreme)	5 (Catastrophic)
Could be expected to cause **limited damage** to the national interest, organisations or individuals by:	Could be expected to cause **damage** to the national interest, organisations or individuals by:	Could be expected to cause **significant damage** to the national interest, organisations or individuals by:	Could be expected to cause **serious damage** to the national interest, organisations or individuals by:	Could be expected to cause **exceptionally grave damage** to the national interest, by:

Handling sensitive and security classified information

NSW – current guidelines

DLMs

Creation and storage
Dissemination and use
Archiving and disposal

Security Classification

Preparation and handling
Removal and auditing
Copying, storage and destruction
Physical transfer

PSPF

DLMs/Security Classification

Protective markings
Access
Use
Storage
Carry
Transfer
Transmit
Official travel
Disposal

Next steps

Consult with Working Group about:

- Security classifications (PROTECTED and above)
- Handling guidelines for DLMs and Security Classifications
- email Protective Marking Standard
- Resources
  - an electronic training module
  - a user-friendly, web-based app
  - a ‘memory jogger’ reference document that summarises the key points of the Guidelines
  - Other suggestions welcome
- Timeframe and costs for implementation

Approvals

- Obtain endorsement of Guidelines from ICT Digital Leaders Group and Secretaries Board
- Issue Department of Customer Service Circular

Transition timeline - Commonwealth

	1 October 2018	1 January 2019	1 October 2020
Implementation stage	**PSPF REFORMS 2018 COMMENCES** Transition to new system commences.	**NEW CLASSIFICATION SYSTEM[3] 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[4] CEASES** Entities **must not** send or receive emails under the old system after this date.
	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 or receive emails using markings under the old system after this date.
Internal (entity) 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 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: only** new system

https://www.protectivesecurity.gov.au/sites/default/files/PSPF-fact-sheet-classification-reforms.pdf

Proposed timeline