



**Office of the Victorian
Information Commissioner**

User Guide

Labelling and Handling Protectively Marked Information

Version 2.0 November 2019

User Guide

Labelling and Handling Protectively Marked Information

Table of Contents

1. Purpose.....	3
2. Audience.....	3
3. Scope	3
4. Use of Terms.....	3
5. What are protective markings?	4
6. Why should I apply protective markings?	4
7. Who determines whether information needs a protective marking?.....	4
8. When do I assess the information?	4
9. What do I do when I receive information (marked or unmarked)?	5
10. What if the information already has an old marking or security classification?.....	5
11. Altering an existing protective marking.....	6
12. Using information that is already protectively marked in your own document.....	6
13. What information should be protectively marked?	6
14. Performing an initial information assessment.....	7
15. Selecting a protective marking (conducting an information security value assessment)	7
16. What markings are available for use under the VPDSF?	8
17. What do each of these markings mean?	8
18. Security classifications	9
19. Cabinet-In-Confidence.....	9
20. Information Management Markers (IMMs)	10
21. Organisation specific markers.....	10
22. Preventing over-classification	10
23. How do I format and apply protective markings?	11
24. What if a document requires more than one protective marking?	12
25. What security measures should I use to protect this information?	12
26. Handling protectively marked information.....	12
ANNEX A.....	13

User Guide

Labelling and Handling Protectively Marked Information

1. Purpose

The '**User Guide**' for labelling and handling protectively marked information provides general guidance on how to manage protectively marked information.

By following the instructions set out in this guide individuals will become familiar with:

- the protective markings that are available for use under the Victorian Protective Data Security Framework (VPDSF);
- general principles on protectively marking information (such as documents and emails); and
- common security measures needed to protect public sector information against unauthorised access or disclosure.

Victorian Public Sector (VPS) organisations should have their own internal policies and procedures addressing the labelling, handling and overall management of protectively marked information. These should be referenced by users in the first instance.

2. Audience

This guide is intended for VPS organisations (including employees, contractors and external parties) that are subject to the protective data security provisions under Part Four of Victoria's Privacy and Data Protection Act (2014).

This guide is designed to support general VPS personnel and information security leads.

3. Scope

This 'User Guide' underpins key elements of the VPDS and should be read in conjunction with:

- other VPDSF material;
- your organisation's security policies and procedures; and
- the Commonwealth's Protective Security Policy Framework (PSPF)

4. Use of Terms

Please refer to the VPDSF Glossary for an outline of terms and associated definitions. A current copy of this is available under the VPDSF Resources on the OVIC website.

5. What are protective markings?

Protective markings are security labels assigned to public sector information. These labels signal the confidentiality requirements of the information, informing particular security controls (e.g. who can access the material or have it disclosed to them).

6. Why should I apply protective markings?

A protective marking acts as a visual signal to those accessing or using the information around the minimum level security measures required when handling, storing, transmitting/ transferring, sharing and disposing public sector information.

7. Who determines whether information needs a protective marking?

The person or organisation responsible for preparing / creating public sector information is best placed to conduct an assessment of the material.

This person or organisation is commonly referred to as 'the originator'.


It is the responsibility of the originator to ensure any recipients of the information, understand how to protect the information. A protective marking helps with this.



8. When do I assess the information?

You should assess the information when you first create, collect or receive it. This includes making sure you assess information contained in word documents, spread-sheets, presentations, emails etc. (including both the body of the email and any attachments).

N.B. The confidentiality requirements of information may change over time. This may be due to the age, currency, amount, intended usage and context of the material. If the confidentiality requirements do change, then you need to conduct a new assessment. This may mean the protective marking may also require updating.



- If you are unsure, contact the originator to clarify, or the information security lead for your organisation.

- contact the person who created the material to understand if there are any confidentiality requirements associated with it
- clarify if it should have a protective marking and if so, what marking is appropriate?
- apply a protective marking based on this discussion and an assessment of potential compromise to the confidentiality of this material
- apply the relevant security measures needed to protect the material



A new scheme was released in February 2019 and VPS organisations have until October 2020 to transition to the new markings. If you are actively using information that already has an old marking or security classification, it may need to be updated or replaced.

If you are actively using the information, you need to re-assess the content using the assessment process set out in this guide, and apply an updated protective marking that reflects the new VPDSF protective marking scheme.

You do not need to do anything if you are not actively using the information. You may consider disposing (archiving or destroying) this material if appropriate. This material can retain its existing marking or security classification.



Freedom of Information | Privacy | Data Protection

11. Altering an existing protective marking

Protective markings must not be adjusted or removed, unless the originator has been consulted and agrees. Before you alter or remove a protective marking, first contact the originator of the information to discuss your specific operating requirements and see what options are available.

N.B. You may see old protective markings from a former scheme. If you are unsure about what the new marking should be or what that marking means, contact the originator of the information to clarify.

12. Using information that is already protectively marked in your own document



If you create a new document that uses or references existing material that is already protectively marked, you must re-assess the overall updated content to see whether there are any increased confidentiality requirements.

If there are increased confidentiality requirements, then a new protective marking may need to be applied to reflect the overall value of the updated content.

N.B. Public sector information that has been protectively marked under a former scheme, must be reassessed under the current VPDSF protective marking scheme, but only if it is being actively used. Documents not in active use do not need to be reassessed, or re-marked.

13. What information should be protectively marked?

Only public sector information needing increased protection should be protectively marked. To help understand the difference between unofficial information and public sector information consider the following definitions:

'Unofficial'

Any information that has **no relation to official activities**, such as a personal correspondence.

Unofficial information does not need to undergo the assessment process.

'Public Sector Information'

Any information (including personal information) obtained, generated, received or held by or for a Victorian public sector organisation **for an official purpose or supporting official activities**.

14. Performing an initial information assessment

To quickly determine whether public sector information requires a protective marking ask yourself:

“What would happen if an unauthorised person accessed this material, or if it was disclosed to someone who wasn’t supposed to see or hear it?” “Would it result in limited forms of harm or damage to government operations, organisations or individuals?” If the answer is:

“Yes” the information may require security measures to protect the confidentiality of the material, and may require a protective marking

“No” then you have determined that a compromise to the confidentiality of the information would be expected to cause **only minor** harm or damage, and is recognised as **OFFICIAL**. Information at this level only requires minimal security measures. (It is not compulsory to label information with an OFFICIAL marker in all instances. This marking can be removed where authorised and appropriate. For example, on documents or material approved for release).

15. Selecting a protective marking (conducting an information security value assessment)

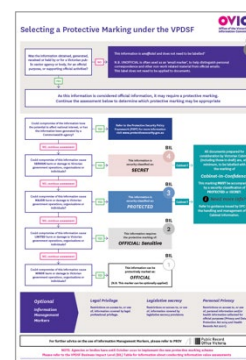
OVIC provides two tools for you to use to help assess public sector information and select a protective marking.

Option 1 –

A light assessment using the **‘Selecting a protective marking’** ready reckoner

This ready reckoner includes a description on what each protective marking means and will help you perform a quick assessment to determine which markings might be appropriate for your information.

Link to resource: [‘Selecting a Protective Marking under the VPDSF’](#).



Option 2 –

A fuller assessment using the **‘VPDSF Business Impact Level (BIL) table’**

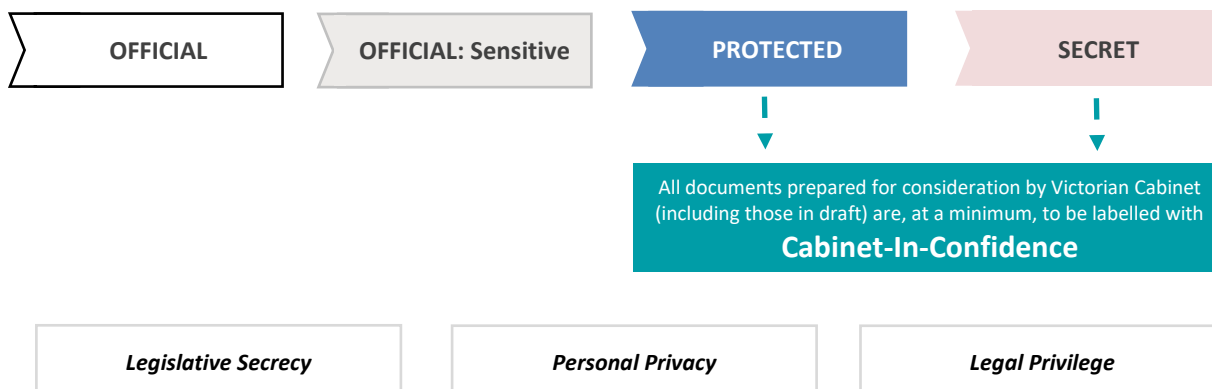
For those looking to substantiate or qualify why they selected a particular protective marking, the VPDSF Business Impact Level (BIL) table can be used to assist in this.

Link to resource: [VPDSF Business Impact Level Table](#)



16. What markings are available for use under the VPDSF?

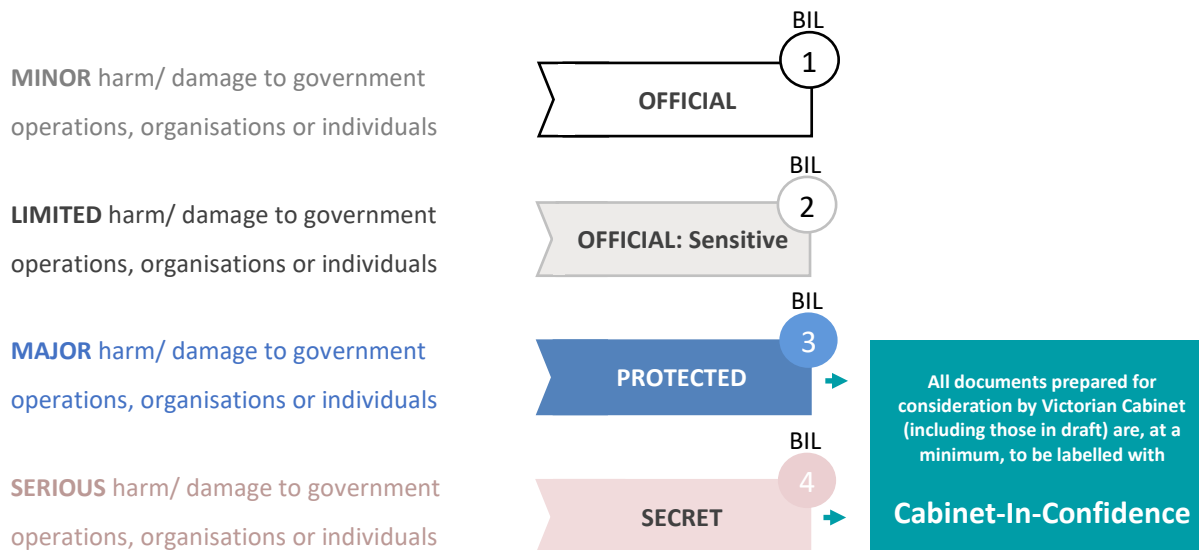
There are a variety of markings available for use under the VPDSF. They include:



** Whilst 'Unofficial' is not recognised as a formal protective marking, it is used for email marking purposes. Unofficial information refers to content that is not related to official work duties or functions.*

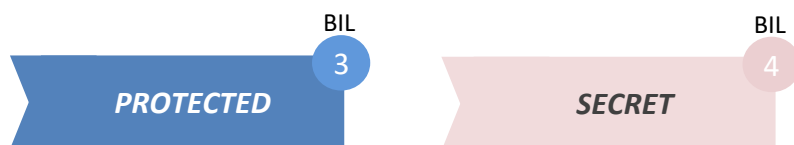
17. What do each of these markings mean?

The main protective markings (depicted below) act as a visual signal of the potential harm or damage that could result if there were a compromise to the confidentiality of the information.



18. Security classifications

There are two security classifications that are used within the Victorian Government. They are:



Security classifications should only be used where compromise of the information could cause major (BIL of 3) or serious (BIL of 4) harm / damage to government operations, organisations or individuals.



For guidance on how to handle TOP SECRET (BIL of 5) information, refer to the Commonwealth Protective Security Policy Framework (PSPF).

19. Cabinet-In-Confidence

Any material marked as 'Cabinet-in-Confidence' must be accompanied by a security classification of PROTECTED or SECRET. When applying these markings to a document, separate them by using two forward slashes. For example:

- **PROTECTED// Cabinet-In-Confidence**, or
- **SECRET// Cabinet-In-Confidence**.

For more information on how to manage and secure 'Cabinet-In-Confidence' information, refer to the [Victorian Cabinet Handbook](#).



20. Information Management Markers (IMMs)

Information Management Markers (IMMs) have been designed to reflect certain access restrictions as well as 'rights property terms' for particular content. While IMMs are not mandatory, they do highlight the 'Rights' property of the information and provide a standard set of terms, ensuring common understanding and consistency, where access or disclosure of information is to be limited. These limitations may be due to:

- disclosure of the material being limited or prohibited by legislation
- special handling requirements of the material
- dissemination controls restricting access

Tabled below are **three commonly recognised IMMs for use across Victorian Government**. Please refer to PROV guidance for more information on IMMs and their use in Victorian Government.

Vic Gov. IMM	Explanation / Basis
Legislative Secrecy	Restriction on access to, or use of, information covered by secrecy provisions under an enactment or legislation
Personal Privacy	Restriction on access to, or use of, personal information and / or health information collected for official purposes (Privacy and Data Protection Act, 2014 and Health Records Act, 2001)
Legal Privilege	Restriction on access to, or use of, information covered by legal professional privilege

21. Organisation specific markers

Some organisations may use markers that are different to those set out under the VPDSF.

These are specific markers generated for **internal use only** and **must be removed or re-labelled prior to releasing**, transmitting or transferring the material outside the organisation.

22. Preventing over-classification

Most public sector information you generate or access will not require special security measures, as compromise of the confidentiality of this material would only be expected to cause minor (BIL 1) harm or damage to government operations, organisations or individuals.



Information assessed at this level, can be left unlabelled, or marked as **OFFICIAL**.

Some informed assessed as **OFFICIAL** information may be suitable for public release. Before publishing, sharing or disseminating information to the public, first check to see if you are authorised to do so.

Refer to your organisation's security policy and procedures, or your information security lead for more information.



It is important that protective markings are only used when needed as inappropriate over-classification could result in:

- access to information being unnecessarily limited or delayed
- onerous administration and procedural overheads, imposing additional costs on the organisation
- people ignoring the importance of protective markings

23. How do I format and apply protective markings?

Once you have assessed the information and determined that it needs a protective marking, you now need to apply these markings to the information. Protective markings can be applied to information in any format and medium. This includes: Paper files / documents / records

- Systems or databases
- Media (magnetic or optical)
- Presentations, maps or visual displays
- Visual media
- Emails¹ *Where possible protective markings are to be applied in the following style and format:*

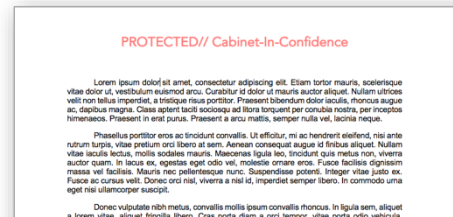
Marking	Description
<i>(all)</i>	5mm high, Bold font, centrally positioned in the header and footer of a document
OFFICIAL	The entire word is capitalised
OFFICIAL: Sensitive	The word ' OFFICIAL ' is capitalised followed by a colon and then the word ' Sensitive ' where the first letter is uppercase, and the following letters are lowercase
PROTECTED	The entire word is capitalised
SECRET	The entire word is capitalised
Cabinet-In-Confidence	' Cabinet-In-Confidence ' should always be accompanied by a security classification of either ' PROTECTED ' or ' SECRET ', separated by two forward slashes when written on a document (i.e. PROTECTED// Cabinet-In-Confidence)

If the media or format of the information restricts labelling options, try to label the protective marking in a clearly visible location or area.

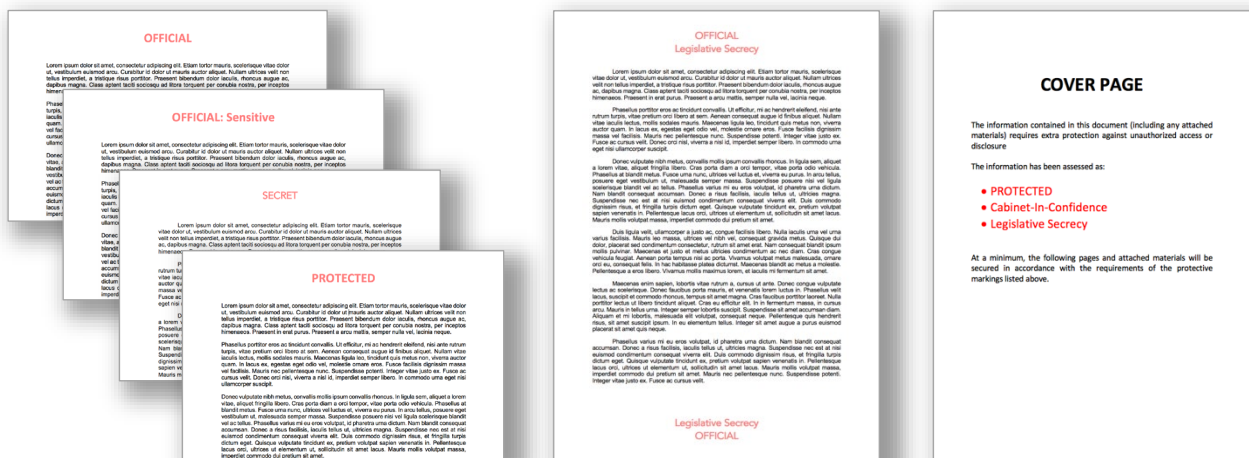
¹ For email marking guidance refer to your organisation's internal policies and procedures and IT Team

24. What if a document requires more than one protective marking?

Sometimes an assessment of the information identifies the need for more than one protective marking. In this instance you should list these on each page of the document, placing the markings in the header and footer of each page, and using two forward slashes to separate the multiple markings.



In addition to this, you can use a cover sheet to signal to the reader that the following pages (including potential attachments) contain protectively marked information and require extra protection. Examples on how to protectively mark a document:



25. What security measures should I use to protect this information?

It is your responsibility to properly secure information that is protectively marked, from the point that it is first created or received, through to when it is no longer being actively used and are ready to dispose of it (either through archival or secure destruction).

Each protective marking informs the need for specific security measures. These security measures are designed to scale in the level of protection they offer, based on the protective marking of the information.

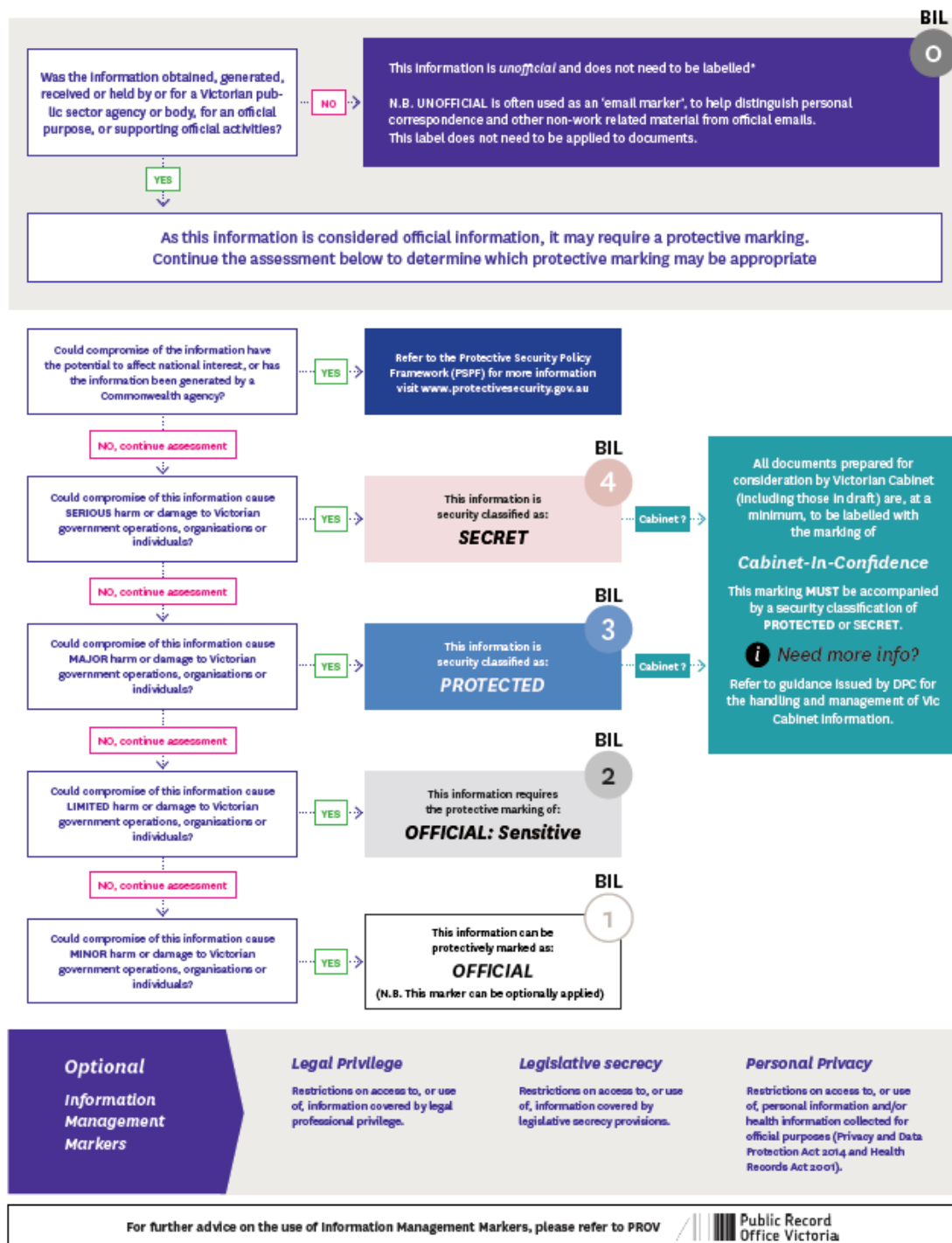
Refer to your organisation's security policies and procedures for further guidance on what security controls are appropriate to secure protectively marked information in your environment.

26. Handling protectively marked information

Organisations will have their own internal security policies and procedures, designed to provide instruction on how individuals are expected to securely handle and manage protectively marked information throughout its lifecycle. Refer to your internal references or guides for more information.

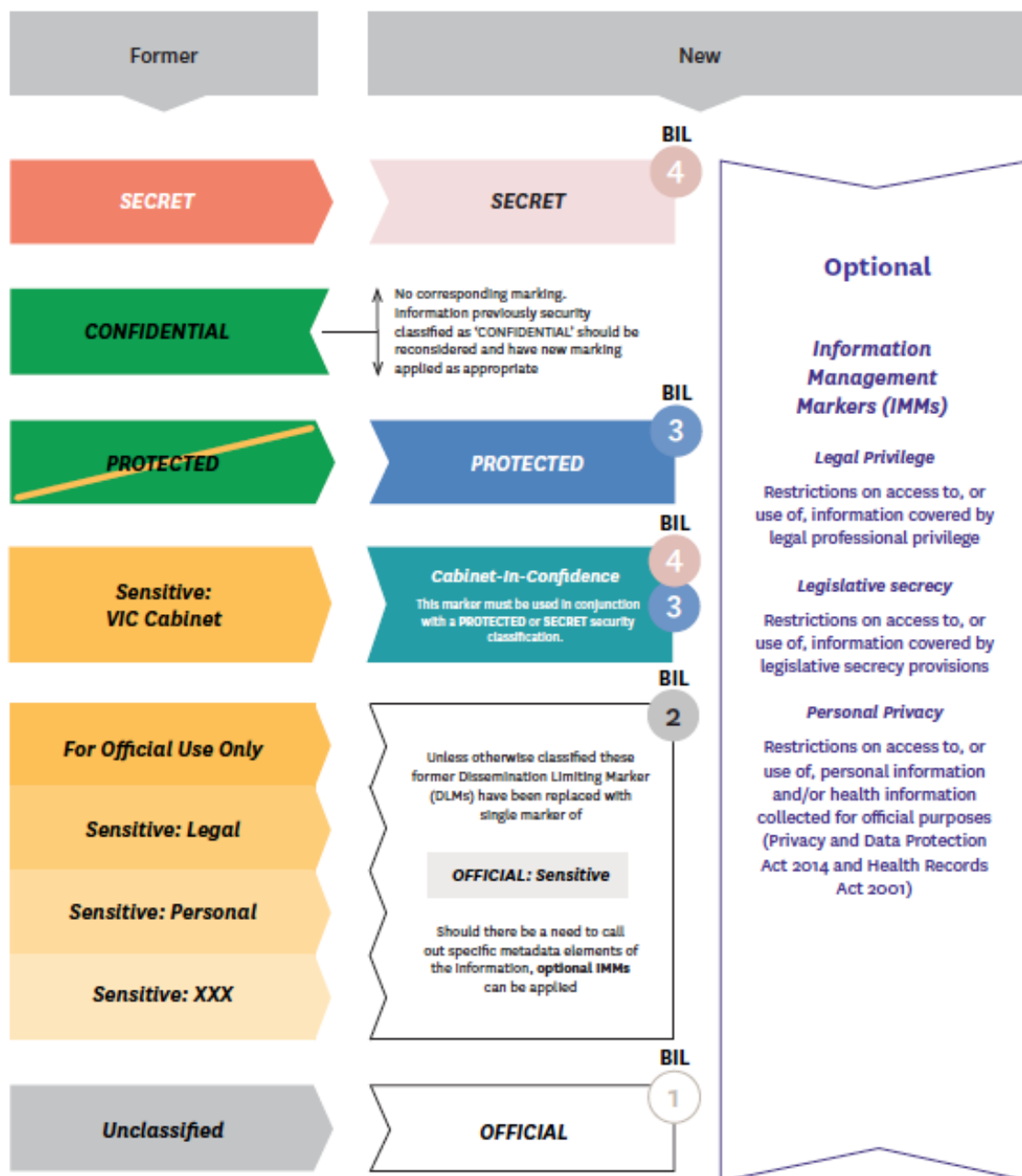
ANNEX A

Selecting a Protective Marking under the VPDSF



NOTE: Agencies or bodies have until October 2020 to implement the new protective marking scheme

Mapping From Old To New Protective Markings



NOTES: 1. Transition timeline from former scheme to new scheme concludes October 2020.
2. Organisations only need to reassess and re-mark information that they are actively using.
3. Please refer to the VPDSF Business Impact Level (BIL) Table for information about conducting information value assessments.