Office of the Victorian
Information Commissioner

# Practitioner Guide:

# Protective Markings

## - 2019 Protective Marking Scheme
## - Protective Markings explained

*(Formerly Chapter 3 of the Information Security Management Collection)*

**Version 2.0 November 2019**

Published by the Office of the Victorian Information Commissioner
PO Box 24274
Melbourne Victoria 3001
First published June 2016
Amended November 2019
Also published on: https://ovic.vic.gov.au
ISBN 978-0-6486723-5-7

## Practitioner Guide Details

| **Protective Markings**<br>*(formerly Chapter 3 of the VPDSF Information Security Management Collection)* | |
|---|---|
| Protective Marking | N/A |
| Approved for unlimited public release? | *Yes – Authorised for release* |
| Release Date | November 2019 |
| Review Date | November 2020 |
| Document Version | 2.0 |
| Authority | Office of the Victorian Information Commissioner (OVIC) |
| Author | Information Security Unit – OVIC |

For further information, please contact the Information Security Unit on security@ovic.gov.au

## Table of Contents

## 1. Background

The Office of the Victorian Information Commissioner (OVIC) issues security guides to support the Victorian Protective Data Security Standards (VPDSS). All guidance documents and references are inter-linked and should not be read in isolation.

This document forms part of a suite of supporting security guides of the VPDSS.

## 2. Purpose

Everyone who works with public sector information has an obligation to respect the information that they create, access and use, and are personally accountable for safeguarding this material. In order to do this, all persons need to have an understanding of the security value of public sector information, and the security measures designed to protect the confidentiality, integrity and availability of public sector information.

This document aims to assist Victorian public sector organisations in understanding:

- what information requires a protective marking;
- what are protective markings;
- the definitions that underpin each protective marking; and
- the benefits of using protective markings.

## 3. Audience

This document is intended for Victorian public sector 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 practitioners and information security leads.

## 4. Use of specific terms in this document

Please refer to the *VPDSF Glossary of Protective Data Security Terms* for an outline of terms and associated definitions. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

## 5. Scope

This document directly supports the Victorian Protective Data Security Standards (VPDSS) and informs the foundational steps for the VPDSS Five Step Action Plan[1].

[1] Refer to the VPDSS Five Step Action Plan for further guidance on each of the steps. The Five Step Action Plan sets out five recommended steps helping inform the development of an organisations Protective Data Security Plan and secure its information assets. For more information, refer to VPDSF Resources section of the OVIC website.

### 6. What are protective markings?

Protective markings are security labels assigned to public sector information. They signify the confidentiality requirements of public sector information, determined via an information security value assessment based on the VPDSF Business Impact Level[2] (BIL) table. Protective markings inform the minimum level of protection to be provided throughout the information lifecycle (e.g. during the use, storage, transmission/transfer and disposal).

### 7. What information requires a protective marking?

Information falls into two broad informal categories:

| PUBLIC SECTOR INFORMATION | *UNOFFICIAL* INFORMATION |
|---|---|
| Public sector information means 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.<br>This includes both hard and soft copy information, regardless of media or format.<br>Not all public sector information will require a protective marking, however other security measures may still be required to protect the integrity and availability of this material. | In contrast, *unofficial* information is any information that has no relation to official activities, such as a personal correspondence.<br>Unofficial information does not need to undergo a security value assessment.<br>*'Unofficial'* information has no bearing on official functions and, as such, must not have a protective marking. Applied to it.<br>N.B. Users may see the label of '*unofficial'* applied to emails, to assist with transmission requirements. |
| May require a protective marking ✓ | Must not be labelled with a protective marking ✗ |

### 8. What are the benefits of using protective markings?

Consistent use of protective markings, coupled with the adoption of appropriate security measures, enhances Victorian Government's ability to conduct business in a secure and effective manner.

Protective markings act as an important visual signal to anyone accessing or using the material, informing the minimum-security obligations that need to accompany public sector information.

Protective markings offer an easily identifiable way for information users (visually) and for systems (such as an entity's email gateway) to identify and manage the handling and control of information at different levels.

[2] In order to undertake consistent information security value assessments, organisations should use a common security valuation criteria called Business Impact Levels (BILs). By undertaking this assessment, organisations can determine the appropriate protective marking and the overall security value of public sector information. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

## 9. Protective markings scheme (Victoria)

Under the VPDSF, the following protective markings are recognised -

| PROTECTIVE MARKING | BASIS FOR PROTECTIVE MARKING |
|---|---|
| BIL 1<br>OFFICIAL | This protective marking may be applied to public sector information that requires some form of protection, as compromise of this information may cause **minor** harm/damage to government operations, organisations and/or individuals.<br>Use of this protective marking signals that the material has undergone an information assessment and visually describes its security value to the end user. However, it is recognised that the application of this protective marking (**OFFICIAL**) may not always be appropriate, and as such does not need to be mandatorily applied. |
| BIL 2<br>OFFICIAL: Sensitive | Apply to public sector information where secrecy provisions or enactments apply to the content, or where disclosure of the material may be **limited** or prohibited under legislation.<br>This indicates where compromise of the confidentiality of the information may cause **limited** harm/damage to government operations, organisations and/or individuals. |
| BIL 3<br>PROTECTED | Apply to public sector information where compromise of the confidentiality of the information may cause **major** harm/damage to government operations, organisations and/or individuals. |
| BIL 4<br>SECRET | Apply to public sector information where compromise of the confidentiality of the information may cause **serious** harm/damage to government operations, organisations and/or individuals. |
| Cabinet-in-Confidence | To be applied to Victorian Cabinet information, based on exemptions under the Freedom of Information Act 1982. A document is described as 'Cabinet-In-Confidence' if it is:<br>• an official record of any deliberation or decision of Cabinet<br>• a document that has been prepared by a Minister or on their behalf or by an agency for the purpose of submission for consideration by Cabinet<br>• a document prepared for the purpose of briefing a Minister in relation to issues to be considered by Cabinet<br>• a document that is a draft of, or contains extracts from a document referred to above<br>• a document which refers to any deliberation or decision of Cabinet, other than a document by which a decision of Cabinet was officially published.<br>The marking of 'Cabinet-In-Confidence' must be used in conjunction with a security classification of either PROTECTED or SECRET. |

## 10. *Unofficial* information

Unofficial information refers to content that is unrelated to official work duties or functions. Content in this category has zero (0) business impact, as it would not be expected to cause harm or damage to government operations, organisations or individuals.

A label of 'unofficial' must not to be applied to public sector information that is of an official nature. Whilst 'unofficial' is not recognised as a formal protective marking, it is used for email marking purposes in some organisation's email systems.

## 11. Information marked as OFFICIAL

The majority of general or routine public sector information will be assessed as **OFFICIAL**.

Some informed assessed as **OFFICIAL** information may be suitable for public release. Organisation's security policy and procedures should outline authorisation or approval processes surrounding the publication, sharing or disseminating of this type of information to the public.

## 12. Information marked as OFFICIAL Sensitive

Where information compromise would have some limited damage but does not warrant a security classification, that information is considered **OFFICIAL: Sensitive**. This includes information where secrecy provisions or enactments apply to the content, or where disclosure of the material may be limited or prohibited under legislation.

## 13. Security classifications

A security classification signals heightened confidentiality requirements of public sector information.

Information marked with a security classification has undergone an information security value assessment and has achieved a BIL of 3 or above. There are two security classifications used within Victorian Government. They are:

BIL
3
PROTECTED
BIL
4
SECRET

The security classifications of **PROTECTED** and **SECRET** reflect the operating requirements of Victorian Government and align with the Commonwealth Protective Security Policy Framework (PSPF) classification scheme.

The security classification of **TOP SECRET**[3] is not referenced as an available protective marking for use under the VPDSF. If an organisation assesses its material as requiring a security classification of TOP SECRET, guidance should be sought from the Commonwealth PSPF[4] on the management of this material.

[3] The security classification of TOP SECRET is not referenced as an available protective marking for use under the VPDSF. Please refer to the Commonwealth Protective Security Policy Framework (PSPF) for more information

[4] For more information on the Commonwealth protective marking scheme, refer to the Protective Security Policy Framework (PSPF)

## 14. Information Management Markers (IMMs)

Information Management Markers (IMMs) have been designed to reflect 'rights properties' for particular content and can inform access restrictions.

While IMMs are not mandatory, they are metadata indicators that provide a standard set of terms ensuring common understanding and consistency where access or disclosure of information is to be limited as:

- disclosure of the material is limited or prohibited by legislation;
- special handling of the material is required; and
- dissemination of the material needs to be controlled.

Depending on the content, some information may require multiple IMMs. In these instances, organisations that are using IMMs should apply each required marker as appropriate.

Within Victorian Government, the following IMMs are provided by PROV. These are the most common markers for use by the VPS. The basis of these IMMs may vary slightly from those at the Commonwealth level, as Victorian legislation used to inform these markings is different.

Under the VPDSF and PROV guidance, the following Information Management Markers (IMMs) are commonly recognised:

| Vic Gov. IMM | Explanation |
|---|---|
| ***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 |

Please refer to PROV guidance for more information on IMMs and their use in Victorian Government.

## 15. Caveats

Caveats indicate that public sector information has special requirements in addition to those identified by a protective marking, further restricting access to the material. Caveats cannot be applied to 'Unofficial' material.

### 15.1. Different Levels of Caveats

There are three levels of caveats:

- **Commonwealth**– most commonly found on information relating to material that could impact the national interest (Inc. national security). Caveats at a Commonwealth level must be used in conjunction with a security classification.
- **Victoria Government** – authorised caveats only (see table below) and must be used in conjunction with a security classification; and

- **Organisation specific** – internal application and use only. They should be removed from the information prior to transfer or transmission outside the organisation.

### 15.2. Caveats for use across Victorian Government

The main caveat approved for use across the VPS is **Cabinet-In-Confidence**. It is not stand-alone protective marking and must be used in conjunction with a security classification of **PROTECTED** or **SECRET**.

### 15.3. Access to Caveat information

Access to caveat information is only available to those who are:

- appropriately screened/security cleared;
- have been briefed about the security value[5] of the particular information; and
- have been informed of any special handling or management conditions relating to that information.

### 15.4. Four types of Caveats

The following four types of caveats have been authorised for use within Victorian Government:

| VICTORIAN CAVEATS | BASIS FOR THE CAVEAT |
|---|---|
| Eyes Only (EO) | The 'Eyes Only' marking indicates that access to information is restricted to certain:<br>Roles (e.g. Ministers);<br>Entities (e.g. Independent Broad-based Anti-Corruption Commission); or<br>where employees are engaged in sensitive interagency projects (e.g. highly sensitive joint projects between Victoria Police and Corrections Victoria personnel).<br>Any information marked 'Eyes Only' cannot be passed to or accessed by those who are not listed in the marking. |
| Releasable to | The caveat 'releasable to' identifies information that has been released or is releasable to the indicated body or group. |
| Special handling caveat | A special-handling caveat is a collection of various indicators such as operation codewords, instructions to use particular communications channels and EXCLUSIVE FOR (named person). |

[5] Refer to the VPDSF Practitioner Guide: Assessing the Security Value of Public Sector Information for more information. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

| | |
|---|---|
| Accountable material | If strict control over access to, and movement of, particularly sensitive information is required, originators can make this information 'Accountable Material'. What constitutes 'Accountable Material' will vary from organisation to organisation, but could include budget papers, tender documents and sensitive ministerial briefing documents. Accountable documents are subject to strict conditions including labelling, individual reference and copy numbers, warnings relating to copy restrictions, transfer, receipting and registration of the material. |

## 16. Victorian Cabinet documentation

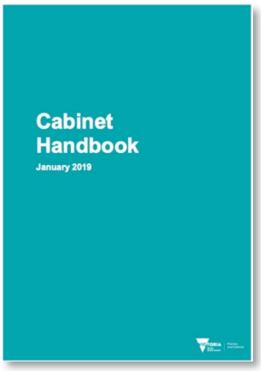
Information used by Victorian Cabinet to formulate policy and make decisions requires special protective security measures. This is because Cabinet material (unlike other public sector information) belongs to the particular government of the day that has created them. They are integral to the process by which government makes decisions and they constitute the record of those decisions.

Unauthorised and/or premature disclosure of Cabinet documentation (including draft documentation) undermines the convention of Cabinet confidentiality.

This confidentiality extends to preserving a Minister's actual or proposed position on Cabinet matters. In order to preserve this convention, it is essential that security measures are applied when handling, transmitting and/or storing this information.

### 16.1. Victorian Cabinet Handbook

The Victorian Cabinet Handbook requires all Victorian Cabinet information to be labelled with the protective marking of 'Cabinet-In-Confidence'. This marking is a default marking for material that has met one or more of the Victorian Cabinet criteria.



Cabinet Handbook

January 2019

Based on exemptions under the Freedom of Information Act 1982, a document is deemed to be 'Cabinet-In-Confidence' (CIC) if it is considered to be:

- an official Record of any deliberation or decision of Cabinet;
- a document that has been prepared by a Minister or on their behalf or by an agency for the purpose of submission for consideration by Cabinet;
- a document prepared for the purpose of briefing a Minister in relation to issues to be considered by Cabinet;
- a document that is a draft of, or contains extracts from a document referred to above; or
- a document which refers to any deliberation or decision of Cabinet, other than a document by which a decision of Cabinet was officially published.

Refer to the Victorian Government Cabinet Handbook[6] and for more information on managing this type of information.

[5] Victorian Government Cabinet Handbook – January 2019

### 16.2. ‘Cabinet-In-Confidence’

Whilst the VPDSF protective marking scheme aligns with the Australian Government Security Classification System (October 2018) it takes into account the unique operating requirements of the Victorian Cabinet office and the Victorian Cabinet Handbook5. The retention of the protective marking of ‘Cabinet-In-Confidence’ distinguishes the VPDSF protective marking scheme from the current Commonwealth scheme outlined under the PSPF.

Given this VPS context, all documents prepared for consideration by Victorian Cabinet (including those in draft) are, at a minimum, be marked with ‘Cabinet-In-Confidence’, coupled with an appropriate security classification of either **PROTECTED** or **SECRET**. In practice, Victorian generated Cabinet information must be protectively marked as either:

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

These markings reflect the minimum controls needed for the protection of Victorian Cabinet documentation. For more information on these controls, refer to the Victorian Cabinet Handbook.

OVIC recognises that updates to an organisation’s systems and processes to reflect this updated protective marking scheme may take some time, however planning for this transition should already be under way.

## 17. Organisation specific markings (non-standard markings)

Organisation specific markings can only be used within the agency or body.
Organisations who use non-standard markings must change/remove these markings before distributing or transferring this information externally.

## 18. Public releasable content

‘Public’ or ‘Approved for public release’ are not protective markings.

They are terms used to describe information that has been approved for unlimited public release, in accordance with the authorising environment of the originating organisation.

Information assessed at this level may be labelled as being ‘*authorised for release*’ or left unmarked.

## 19. Protectively marked information from another organisation

It is essential that users understand and respect the protective marking applied by the originator of the information. This includes information generated by:

- Local Councils or Shires;
- State or Territory agencies;
- Commonwealth Departments or agencies;
- Foreign Governments; and
- Private industry bodies.

If an organisation receives information labelled with an unfamiliar protective marking, they should contact the originator of that material as there may be specific security obligations imposed by that marking.

## 20. Commonwealth information

While the Victorian and Commonwealth protective marking schemes are similar, the Commonwealth PSPF does describe specific protective markings available for use by Commonwealth departments and agencies.

It is unlikely that these protective markings will be referenced by Victorian public sector organisations, however on the rare occasion that this may be required, organisations should refer to the PSPF for further information on the handling and management of this material.

*Please note:* Information of a 'national interest' may also bear a protective marking of PROTECTED and SECRET, not just at TOP SECRET.

## 21. Other State or Territory information

Where another State or Territory has generated information and applies a protective marking, the marking and any accompanying security controls must be respected by the receiving organisation in Victoria. Contact the originator of the information if there are any questions relating to the management or handling of that information.

## 22. Foreign Government information

Where security classified information is provided under a bilateral agreement, foreign government information (FGI) is to be given the equivalent protective marking. FGI cannot be distributed outside the conditions of these agreements. For more information, refer to the FGI instructions under the PSPF.

## 23. Private industry body markings

Information produced by a private sector entity may not have a protective marking. More commonly material generated from a private sector entity is either unlabeled or includes a commercially recognised label (e.g. Commercial in Confidence).

VPS organisations receiving material from private sector entities should contact the originator of the information to help inform what protective marking may be required for the material as it is now in the custody of a Victorian public sector organisation. This is also an opportunity to clarify if there are any additional security requirements relating to the management or handling of the information.

Where private sector entities generate information on behalf of a Victorian public sector organisation (i.e. contractor, consultants, etc.), these entities should refer to the engaging organisation's security policies and procedures that outline their protective marking requirements.

## 24. Unfamiliar markings

If a Victorian Government organisation receives information labelled with an unfamiliar protective marking, they should contact the originator of that material as there may be specific security obligations and controls imposed by that marking.

## 25. Information protectively marked under a former scheme

Information that has been protectively marked under a former scheme is referred to as 'legacy' information or sometimes 'legacy classified information'.

Only public sector information that is being actively used by a Victorian public sector organisation needs to undergo an updated information security value assessment to determine its current value. This updated assessment will help organisations apply the appropriate protective markings needed for the information, reflecting the new protective marking scheme.

*VPDSF Practitioner Guide: Assessing the Security Value of Public Sector Information* sets out the information security value assessment process that organisations are expected to follow.

It is important to note that any information that is not being actively used or has already been archived, does not require a re-assessment. This information can retain its former protective marking(s) or security classification and be appropriately stored or securely destroyed as required.

Sample legacy markings may include:

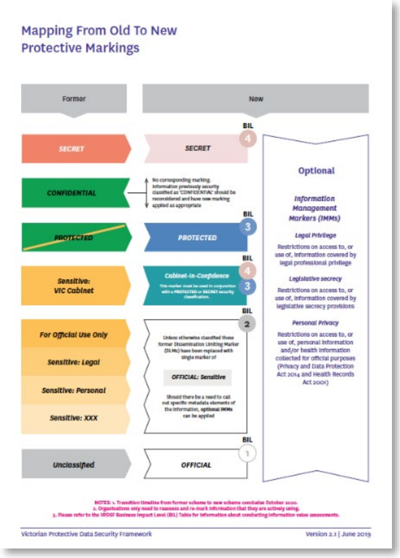
- In-Confidence or X-In-Confidence
    - N.B. This excludes Cabinet-In-Confidence as this is a current protective marking
- Restricted
- Highly Protected
- UNCLASSIFIED / Unclassified
- CONFIDENTIAL
- For Official Use Only
- Sensitive: Vic Cabinet
- Sensitive: Legal
- Sensitive: Personal

## 26. Indicative mapping from old to new protective markings

To assist organisations adopt the new protective marking scheme, OVIC has produced a ready reckoner that provides an indicative mapping from the old protective marking scheme to the new one.

Organisations should still perform an information security value assessment of their public sector information when actively using this material, referencing this ready reckoner as guidance.

A copy of this ready reckoner is provided *Appendix B* of this guide.



Mapping From Old To New Protective Markings

No corresponding marking. Information previously security classified as 'CONFIDENTIAL' should be reconsidered and have new marking applied as appropriate

This marker must be used in conjunction with a PROTECTED or SECRET security classification.

Unless otherwise classified these former Dissemination Limiting Marker (DLMs) have been replaced with single marker of OFFICIAL: Sensitive

Should there be a need to call out specific metadata elements of the information, optional IMMs can be applied

Legal Privilege

Restrictions on access to, or use of, information covered by legal professional privilege

Legislative secrecy

Restrictions on access to, or use of, information covered by legislative secrecy provisions

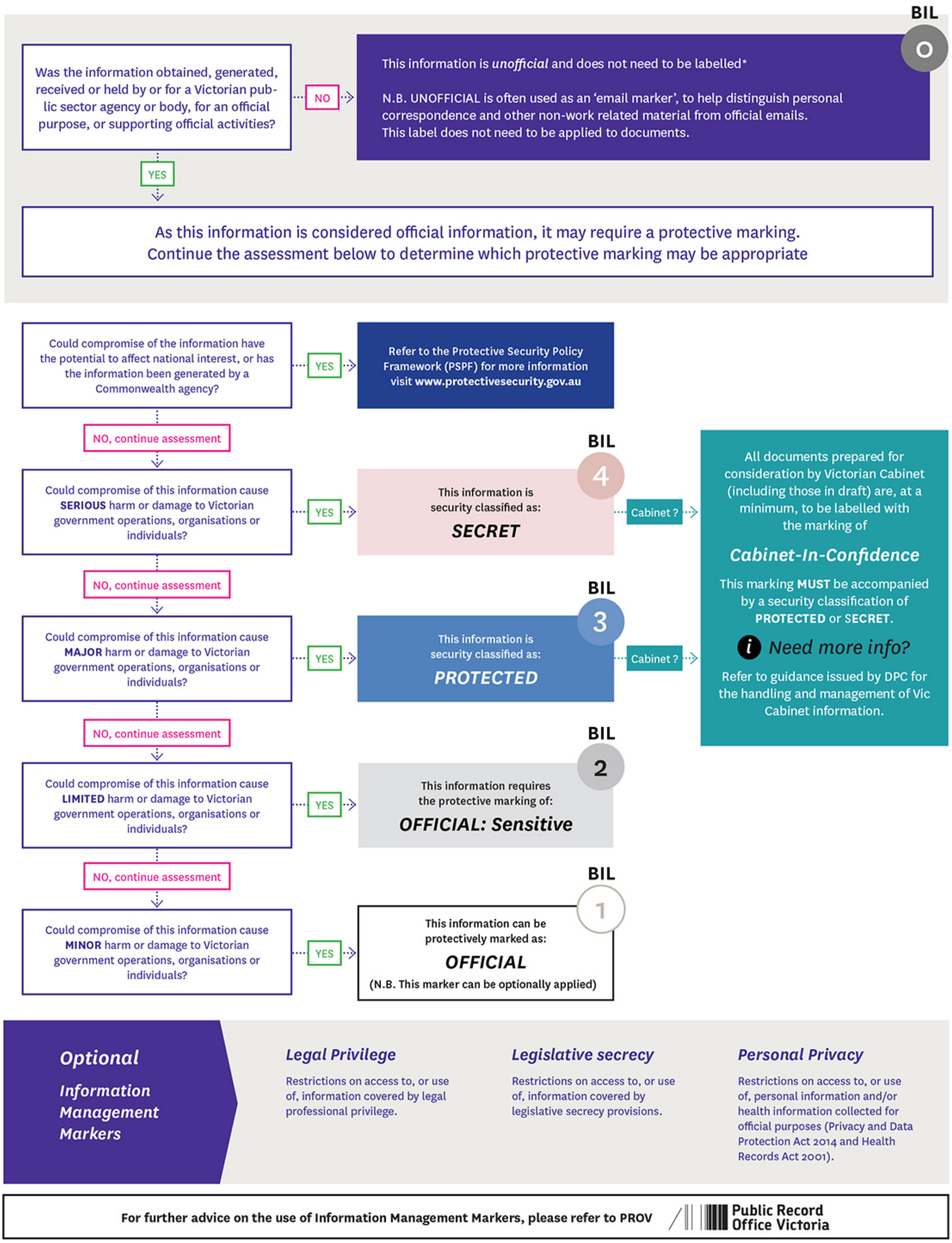
Personal Privacy

Restrictions 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)

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.

Victorian Protective Data Security Framework
Version 2.1 | June 2019

## Appendix A – Ready reckoner: Selecting a protective marking under the VPDSF



Was the information obtained, generated, received or held by or for a Victorian public sector agency or body, for an official purpose, or supporting official activities?

NO → BIL O

This information is *unofficial* and does not need to be labelled*

N.B. UNOFFICIAL is often used as an 'email marker', to help distinguish personal correspondence and other non-work related material from official emails. This label does not need to be applied to documents.

YES ↓

As this information is considered official information, it may require a protective marking. Continue the assessment below to determine which protective marking may be appropriate

Could compromise of the information have the potential to affect national interest, or has the information been generated by a Commonwealth agency?

YES → Refer to the Protective Security Policy Framework (PSPF) for more information visit **www.protectivesecurity.gov.au**

NO, continue assessment ↓

Could compromise of this information cause **SERIOUS** harm or damage to Victorian government operations, organisations or individuals?

YES → BIL 4 This information is security classified as: ***SECRET*** ⋯ Cabinet ? →

NO, continue assessment ↓

Could compromise of this information cause **MAJOR** harm or damage to Victorian government operations, organisations or individuals?

YES → BIL 3 This information is security classified as: ***PROTECTED*** ⋯ Cabinet ? →

NO, continue assessment ↓

Could compromise of this information cause **LIMITED** harm or damage to Victorian government operations, organisations or individuals?

YES → BIL 2 This information requires the protective marking of: ***OFFICIAL: Sensitive***

NO, continue assessment ↓

Could compromise of this information cause **MINOR** harm or damage to Victorian government operations, organisations or individuals?

YES → BIL 1 This information can be protectively marked as: ***OFFICIAL*** (N.B. This marker can be optionally applied)

All documents prepared for consideration by Victorian Cabinet (including those in draft) are, at a minimum, to be labelled with the marking of

***Cabinet-In-Confidence***

This marking **MUST** be accompanied by a security classification of **PROTECTED** or **SECRET**.

ℹ *Need more info?*

Refer to guidance issued by DPC for the handling and management of Vic Cabinet information.

***Optional Information Management Markers***

***Legal Privilege***

Restrictions on access to, or use of, information covered by legal professional privilege.

***Legislative secrecy***

Restrictions on access to, or use of, information covered by legislative secrecy provisions.

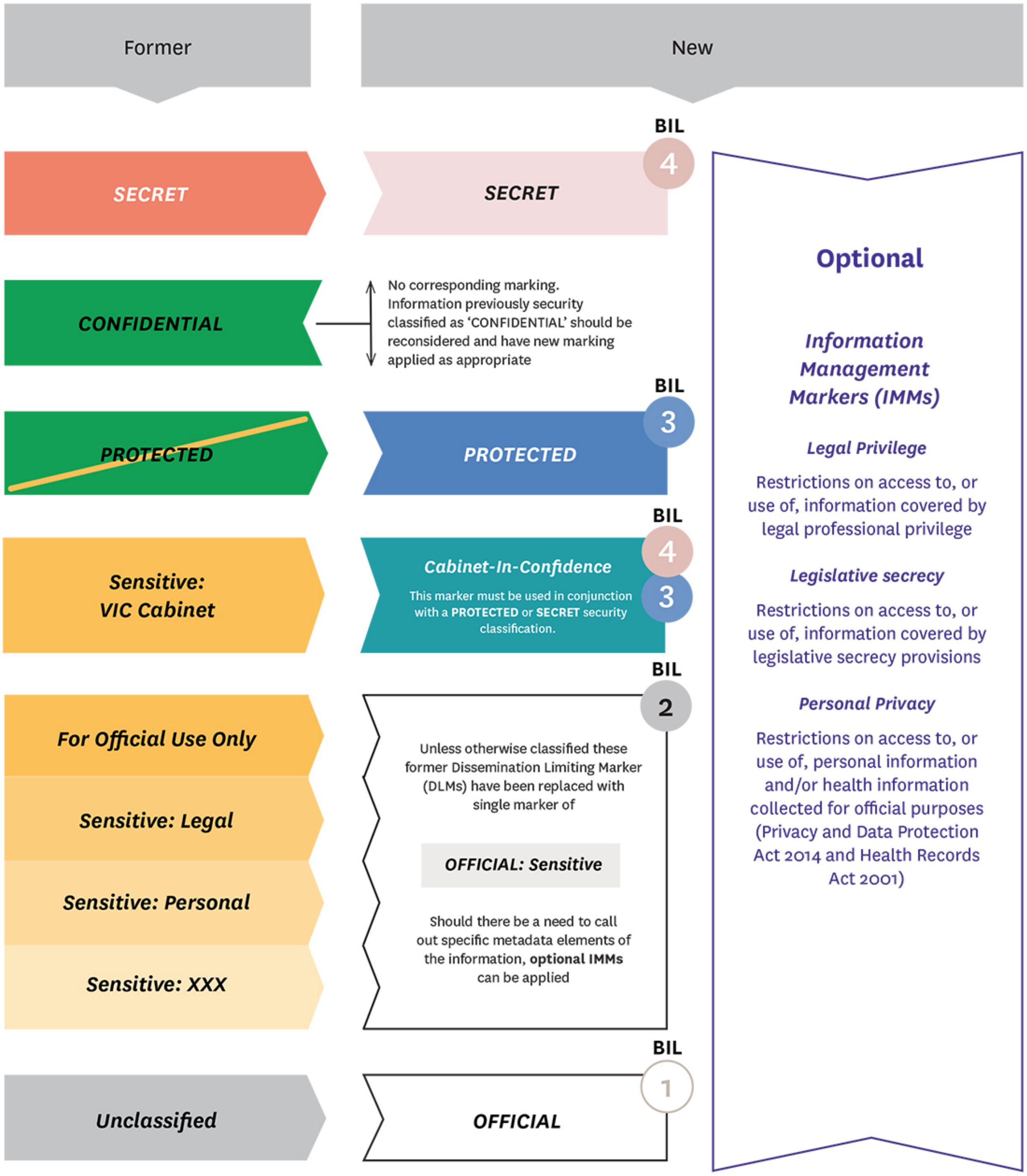
***Personal Privacy***

Restrictions 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).

**For further advice on the use of Information Management Markers, please refer to PROV** Public Record Office Victoria

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

## Appendix B –Indicating Mapping from old to new – protective markings



Former

New

BIL

*SECRET*

4

*SECRET*

*CONFIDENTIAL*

No corresponding marking. Information previously security classified as 'CONFIDENTIAL' should be reconsidered and have new marking applied as appropriate

BIL

~~*PROTECTED*~~

3

*PROTECTED*

BIL

*Sensitive: VIC Cabinet*

4

3

*Cabinet-In-Confidence*

This marker must be used in conjunction with a **PROTECTED** or **SECRET** security classification.

BIL

*For Official Use Only*

*Sensitive: Legal*

*Sensitive: Personal*

*Sensitive: XXX*

2

Unless otherwise classified these former Dissemination Limiting Marker (DLMs) have been replaced with single marker of

*OFFICIAL: Sensitive*

Should there be a need to call out specific metadata elements of the information, **optional IMMs** can be applied

BIL

*Unclassified*

1

*OFFICIAL*

**Optional**

***Information Management Markers (IMMs)***

***Legal Privilege***

Restrictions on access to, or use of, information covered by legal professional privilege

***Legislative secrecy***

Restrictions on access to, or use of, information covered by legislative secrecy provisions

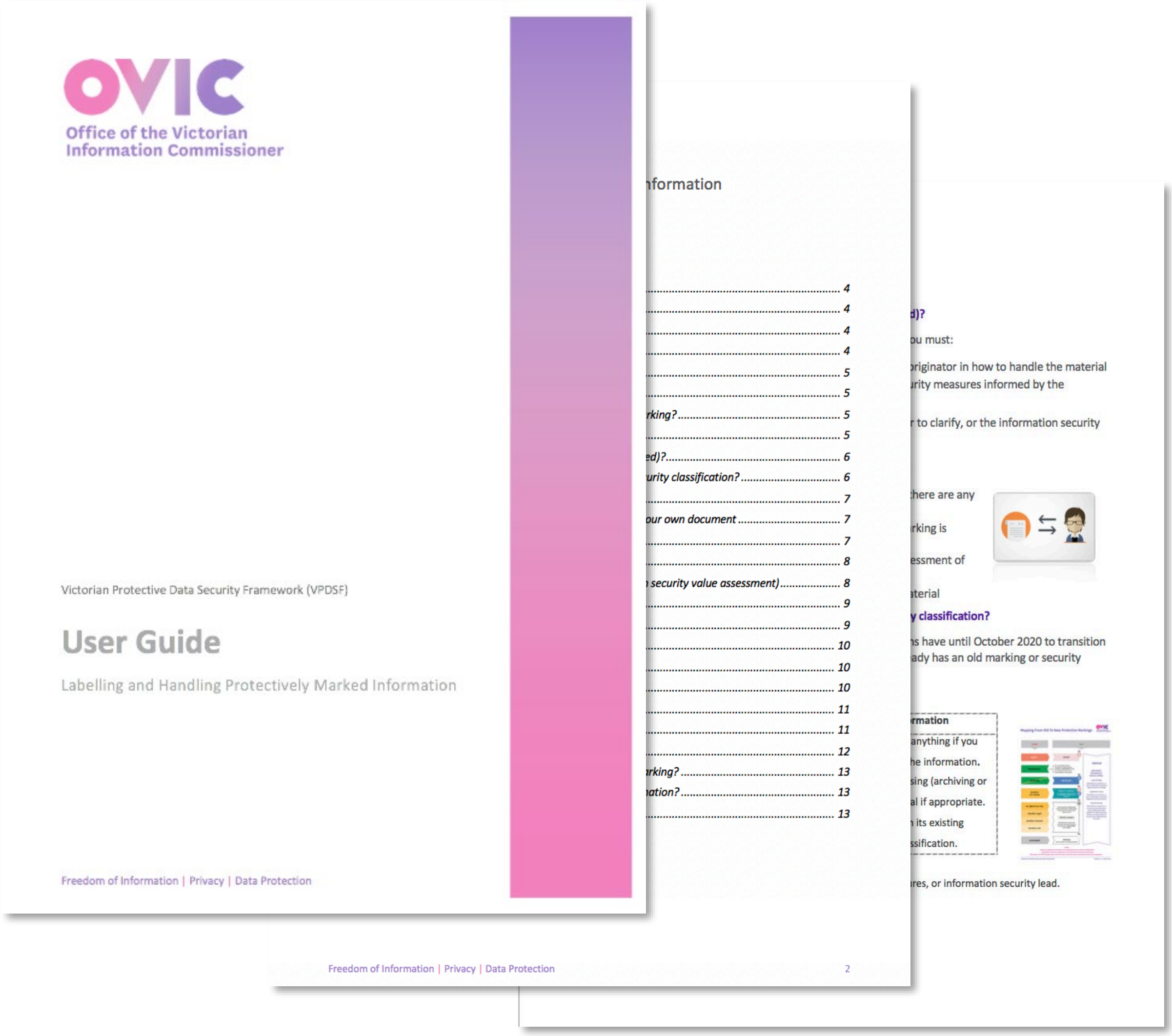
***Personal Privacy***

Restrictions 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)

**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.**

## Appendix C–User Guide – Labelling and Handling Protectively Marked Information

For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.



OVIC
Office of the Victorian Information Commissioner

Victorian Protective Data Security Framework (VPDSF)

User Guide

Labelling and Handling Protectively Marked Information

Freedom of Information | Privacy | Data Protection

nformation

Freedom of Information | Privacy | Data Protection 2

d)?

ou must:

riginator in how to handle the material
rity measures informed by the

r to clarify, or the information security

here are any
rking is
essment of
aterial

y classification?

s have until October 2020 to transition
ady has an old marking or security

rmation
anything if you
he information.
sing (archiving or
al if appropriate.
 its existing
ssification.

res, or information security lead.