Office of the Victorian Information Commissioner

Technical Specification:

Email Protective Markings

(Utilising EPMS 2018.4)

Version 1.1 October 2020

Freedom of Information | Privacy | Data Protection

Published by the Office of the Victorian Information Commissioner
PO Box 24274
Melbourne Victoria 3001
First published October 2020
Also published on: https://ovic.vic.gov.au

You are free to re-use this work under a Creative Commons Attribution 4.0 licence, provided you credit the State of Victoria (Office of the Victorian Information Commissioner) as author, indicate if changes were made and comply with the other licence terms. The licence does not apply to any branding, including Government logos.

Resource Details

VPDSF Technical Specification: Email Protective Markings ***(utilising EPMS 2018.4)***	
Protective Marking	OFFICIAL
Approved for unlimited public release	Yes – Authorised for release
Release Date	October 2020
Review Date	October 2021
Document Version	1.1
Authority	Office of the Victorian Information Commissioner (OVIC)
Author	Information Security Unit – OVIC

Change Log

Version	**Publish Date**	**Amendments in this version**
1.0	October 2020	Original Version
1.1	October 2020	**Section 9:** Added *"Note: If there is a conflict between rules in this specification and rules in the EPMS 2018.4, please contact OVIC for further advice."*
		Appendix A: Updated all X-protective-marking samples with a "Folding white space", i.e. a space before character on the second and further lines. See RFC5322, Para 3.2.2.

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

Table of Contents

1. Background

The Office of the Victorian Information Commissioner (**OVIC**) issues technical specifications 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 material of the VPDSS.

This technical specification for email protective markings (the **specification**) outlines minor departures from the Commonwealth Government requirements as defined in the Protective Security Policy Framework (**PSPF**) and the Email Protective Marking Standard (**EPMS**)[1] 2018.4.

2. Purpose

This document defines the technical implementation of protective markings for emails, for Victorian Public Sector (**VPS**) organisations.

3. Audience

This document is intended for VPS organisations (including employees, contractors and external parties) and industry stakeholders that are subject to the protective data security provisions under Part Four of Victoria's Privacy and Data Protection Act (2014) or are looking to implement the protective marking requirements within a VPS organisation.

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.

The below acronyms are used in this document.

Acronym	Full text	Description
ABNF	Augmented Backus–Naur form	Used to describe a formal system of a language to be used as a bidirectional communications protocol.
EPMS	Email Protective Marking Standard	A standard approach for Commonwealth agencies and bodies in implementing protective markings on emails. This includes ensuring the protective markings accurately reflect the information in the subject, body and attachments of emails.

[1] The Email Protective Marking Standard (EPMS) can be found in Protective Security Policy Framework, Policy 8 - Annex G (V2018.4)

5. Related material

Guidance	Resource	Description
Victorian Protective Data Security Framework (VPDSF)	Practitioner Guide: Identifying and Managing Information Assets V2.0[2]	This document provides a structured approach for Victorian public sector organisations to: • identify what information assets they have (conduct an information review); • articulate and define their information assets; and • collectively record and manage their information assets (establish an information asset register).
	Sample Information Asset Register (IAR) Template V2.0[2]	An Information Asset Register (IAR) is a tool that organisations can use to record collections of information (information assets) regardless of media or format. This resource provides a sample IAR template.
	Practitioner Guide: Assessing the Security Value of Public Sector Information V2.0[2]	This document aims to assist organisations by: • providing guidance about assessing public sector information using a consistent impact assessment tool (taking the form of Business Impact Levels – BILs[3]); • contextualising the VPDSF BILs in line with the organisations specific operating requirements; • determining the overall security value of public sector information; • identifying the appropriate protective marking for the information; and • understanding if additional security measures are required to protect public sector information (beyond those security measures already informed by the protective marking).

[2] All VPDSF resources listed in this table link to the VPDSF Resources page on the OVIC website

[3] Business Impact Levels (BILs) describe scaled impacts which would be expected to cause harm or damage to government operations, organisations or individuals, if there were a compromise of the confidentiality, integrity and/or availability of public sector information.

Guidance	Resource	Description
	VPDSF Business Impact Level Table v2.1[2]	Business Impact Levels (BILs) are used to assess the security value of public sector information. The BIL table presents quantitative measures of scaled impacts, that describe the potential impact arising from a compromise of the - • Confidentiality; • Integrity and / or • Availability. of public sector information.
	Practitioner Guide: Protective Markings V2.0[2]	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.
	Protective Markings Flowchart (Ready Reckoner) and Mapping Old to New Protective Markings V2.1 [2]	A resource for end users, which includes a flowchart prompting the selection of a protective marking and an indicative mapping ready reckoner, helping users transition from the old protective markings to the new scheme.
	User Guide – Handling Protectively Marked Information V2.0[2]	The 'User Guide' for labelling and handling protectively marked information provides general guidance on how to manage protectively marked information.
Protective Security Policy Framework (PSPF)	PSPF Policy 8 – Annex G – Commonwealth Email Protective Marking Standard	The Email Protective Marking Standard (EPMS) 2018.4, outlined under the PSPF.
Information Security Manual (ISM)	Guidelines for Email Management (June 2020)	Technical guidelines outlining controls for email management and protective marking implementation.

Guidance	Resource	Description
Digital Transformation Agency (DTA)	Protected Utility Blueprint	The Blueprint is a design for a secure, modern desktop based on Microsoft Office 365. It provides support for government agencies to standardise the way they work, and to communicate and collaborate without compromising security.

6. Scope

This document directly supports the VPDSS Information (Standard 2) and Information Communication Technology security standards (Standards 11).

7. Email Protective Markings

7.1. What are email protective markings?

Protective marking(s) used to indicate the highest confidentiality protection requirements of any part or component of the email message (including attachments).

7.2. Why should you apply protective markings to emails?

A standard approach to, and implementation of, email protective markings supports processes and systems (such as an entity’s email gateway) controlling the flow of information in and out of the entity. For email recipients, it also signals the handling protections needed to safeguard the information, as visually represented by the email marking.

8. Implementation

There are three options (two core and one supplementary) to consider when implementing email protective markings. Organisations must implement at least one of the core options outlined below, with the supplementary option highly recommended.

Core Options	Description	Implementation Instructions	Notes
Internet Message Header Extension	The protective marking is included in an Internet Message Header Extension, using the specified syntax.	The Internet Message Header Extension marking is the preferred implementation approach, as it enables parsing by email agents (gateways and servers)[4]. Depending on the implementation of a particular solution, organisations may implement technical controls commensurate with the protective marking.	Both options can be used in conjunction with one another in a single email message, so long as the protective marking is consistent across both.
Subject Field Marking	The protective marking is embedded in the Subject Field, using the specified syntax.	Where an internet message header extension is not possible, protective markings should be placed in the Subject Field of an email. Positioning of marking at the discretion of the organisation[5].	

Supplementary Option	Description	Implementation Instructions	Notes
Email Body Markings	The protective marking is embedded in the email body[6].	This is especially important if the email is printed, as it is considered a physical document. It highlights to the user that the content and/or attachment(s) require special protections.	The format and text of email body markings is outside the scope of the EPMS 2018 because the EPMS is about machine interpretation of the protective marking and it is simpler for machines to consistently read data from a message header or subject line.

[4] If an email uses both forms of the protective marking, information in the Internet Message Header Extension takes precedence over the Subject Field Marking.

[5] It is recommended that organisations position the marking using the specified syntax at the end of the Subject Field.

[6] Refer to Section 23 of User Guide: Handling Protectively Marked Information for formatting guidance.

8.1. Email protective marking tools

There are several tools that can assist organisations implement email protective marking labels. Alternatively, whilst not ideal, protective markings to the subject field using the specific syntax, can be manually entered by the user.

8.2. A note on implementation of email protective markings

Whilst the ISM outlines security controls[7] that are defined to block emails with inappropriate protective markings, in practice, State and Territory emails should be permitted.

The PSPF notes that "entity arrangements for receiving emails from sources other than non-corporate Commonwealth entities remain the same (e.g. emails from State and Territory entities, corporate Commonwealth entities, and non-government organisations). Gateways will need to accommodate incoming emails from these sources bearing different markings."[8]

9. VPS departure from the EPMS 2018.4

In place of the Augmented Backus–Naur form (ABNF) specifications defined in EPMS 2018.4, VPS organisations should use the following ABNF rules. The following modifications are the only departures from the EPMS 2018.4.

Note: If there is a conflict between rules in this specification and rules in the EPMS 2018.4, please contact OVIC for further advice.

9.1. Modification of the Syntax of the Protective Marking

9.1.1.Internet Message Header Extension: 'X-Protective-Marking' rules

For organisations utilising the Internet Message Header Extension, and sending Victoria Cabinet information, the special handling caveat of '**CABINET-IN-CONFIDENCE**' must be used.

This special handling caveat must be accompanied with a security classification of at least **PROTECTED**.

The structure of the display value in the body of the email should reflect:

X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au,
SEC=PROTECTED,
CAVEAT=SH:CABINET-IN-CONFIDENCE,
ORIGIN=<senderEmailAddress>

9.1.2.Subject header marking rules

In the subject header, the VPS implementation must reflect **CABINET-IN-CONFIDENCE**, accompanied with a security classification of at least **PROTECTED**. The structure of the header should reflect:

[SEC=PROTECTED, CAVEAT=SH:CABINET-IN-CONFIDENCE].

[7] Information Security Manual (ISM) control references 0565 and 1023

[8] PSPF Policy 8 Sensitive and classified Information - Annex G: Email Protective Marking Standard 2018.4 footnote 1

9.1.3. Email body marking rules

CABINET-IN-CONFIDENCE must be embedded in the body of the email message as a display value, accompanied with a security classification of at least **PROTECTED**. The structure of the display value in the body of the email should reflect e.g. **PROTECTED//CABINET-IN-CONFIDENCE** or **SECRET//CABINET-IN-CONFIDENCE**.

9.2. Modification of specifications outlined in EPMS 2018.4

9.2.1. Table 5: Symbols used in regular expression definition

Below is an extract of *Table 5: Symbols used in regular expression definition* for the symbol <caveatValue> as outlined in EPMS 2018.4, with an added <caveatValue> definition of CABINET-IN-CONFIDENCE.

Symbol	Definition
<caveatValue>	**d.** A Special Handling <caveatValue>s is one of: ***[new insertion below, specific to VPS organisations]*** **vi.** CABINET-IN-CONFIDENCE **A.** This marking has been defined by the Victorian Cabinet office for Victorian Cabinet Information[9]

9.2.2. Table 11: ABNF Definition: Caveat literals

The following row should be read in conjunction with the rules defined in *Table 11: ABNF Definition: Caveat literals* of the EPMS 2018.4.

The CABINET-IN-CONFIDENCE name rule, production value and comment is in addition to the rules defined in *Table 11* of the EPMS 2018.4, to allow for the Victorian special handling caveat of CABINET-IN-CONFIDENCE.

Rule name	Production	Comment
cabinet-in-confidence	%d67.65.66.73.78.69.84 "-" %d73.78 "-" %d67.79.78.70.73.68.69.78.67.69	; CABINET-IN-CONFIDENCE

[9] Refer to VPDSF Resources page to access the *VPDSF Practitioner Guide: Protective Markings* for more information on this marker

9.2.3.Table 12: ABNF definition: Caveat rules

Deviation from the EPMS 2018.4 *Table 12: ABNF definition: Caveat rules*, with an additional special-handling caveat of CABINET-IN-CONFIDENCE.

Rule name		Production	Comment
caveat-tag	=	%d67.65.86.69.65.84	; CAVEAT
codeword-caveat	=	codeword ":" one-to-128-safe-text	
foreign-caveat	=	foreign-government ":" one-to-128-safe-text	
release-caveat	=	releasability-indicator ":" (austeo / agao / rel "/" country-codes)	; See Footnote 10 for email system design guidance
handling-caveat	=	special-handling ":" (NATIONAL-CABINET / CABINET / CABINET-IN-CONFIDENCE / orcon / delicate-source / accountable-material / exclusive-for named-person-or-indicator)	; CABINET-IN-CONFIDENCE as a special handling caveat references the rule name as defined in Table 11
caveat-pair	=	codeword-caveat / foreign-caveat / release-caveat / handling-caveat	
caveat	=	caveat-tag "=" caveat-pair	

9.2.4.Table 18: Namespace rules

Deviation from the EPMS 2018.4 Table 18: Namespace rules, with an adjusted namespace-value to reflect Victorian Government.

Rule Name		Production	Comment
namespace-tag	=	%d78.83	; NS
namespace-value	=	"2019.2.1.vic.gov.au"	; case-insensitive. The 2019.2.1 reference in the namespace value refers to the current version of the Victorian Government Protective Marking Scheme
namespace	=	namespace-tag "=" namespace-value	; NS=gov.au

[10] The email system design should consider and manage the difference between the two ‘exclusive-for’ cases: the restrictive AGAO and AUSTEO tags (emails distributed within the system) and the permissive REL (emails distributed to a foreign system).

Appendix A – Examples of emails with Protective Markings applied

Example Email Protective Marking(s)	Syntax
UNOFFICIAL[11]	X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au, SEC=UNOFFICIAL, ORIGIN=<senderEmailAddress> Subject: This is an example subject line [SEC=UNOFFICIAL] **UNOFFICIAL** This is an example message body. Bye, Rachel
OFFICIAL	X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au, SEC=OFFICIAL, ORIGIN=<senderEmailAddress> Subject: This is an example subject line [SEC=OFFICIAL] **OFFICIAL** This is an example message body. Regards, Rachel

[11] The use of email body markings for **UNOFFICIAL** information are optional

Example Email Protective Marking(s)	Syntax
OFFICIAL: Sensitive[12]	X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au, SEC=OFFICIAL:Sensitive, ORIGIN=<senderEmailAddress> Subject: This is an example subject line [SEC=OFFICIAL:Sensitive] **OFFICIAL: Sensitive** This is an example message body. Regards, Rachel
OFFICIAL: Sensitive **Legal Privilege**[13]	X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au, SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege, ORIGIN=<senderEmailAddress> Subject: This is an example subject line [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege] **OFFICIAL: Sensitive** **Legal Privilege** This is an example message body. Regards, Rachel

[12] For protective marking **OFFICIAL: Sensitive**, ABNF has no space between colon and the S, therefore subject line shows as [SEC=OFFICIAL:Sensitive]. If a protective marking is also applied in the body of the email, that marking should read OFFICIAL: Sensitive (i.e. with a space) in line with PSPF policy 8, Requirement 4.

[13] This is an example of an IMM being used in conjunction with the protective marking of **OFFICIAL: Sensitive**

Example Email Protective Marking(s)	Syntax
OFFICIAL: Sensitive//NATIONAL CABINET	X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au, SEC=OFFICIAL:Sensitive, CAVEAT=SH:NATIONAL-CABINET[14], ORIGIN=<senderEmailAddress> Subject: This is an example subject line [SEC=OFFICIAL:Sensitive, CAVEAT=SH:NATIONAL-CABINET] **OFFICIAL: Sensitive//NATIONAL CABINET** This is an example message body. Regards, Rachel
PROTECTED	X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au, SEC=PROTECTED, ORIGIN=<senderEmailAddress> Subject: This is an example subject line [SEC=PROTECTED] **PROTECTED** This is an example message body. Regards, Rachel

[14] **NATIONAL CABINET** caveat commences on 1 December 2020, with implementation by all non-corporate Commonwealth entities (NCCEs) who are required to use this caveat, required by 31 March 2021.

Example Email Protective Marking(s)	Syntax
PROTECTED//CABINET-IN-CONFIDENCE	X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au, SEC=PROTECTED, CAVEAT=SH:CABINET-IN-CONFIDENCE, ORIGIN=<senderEmailAddress> Subject: This is an example subject line [SEC=PROTECTED, CAVEAT=SH:CABINET-IN-CONFIDENCE] **PROTECTED//CABINET-IN-CONFIDENCE** This is an example message body. Regards, Rachel
PROTECTED//CABINET-IN-CONFIDENCE **Personal Privacy**	X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au, SEC=PROTECTED, CAVEAT=SH:CABINET-IN-CONFIDENCE, ACCESS=Personal-Privacy, ORIGIN=<senderEmailAddress> Subject: This is an example subject line [SEC=PROTECTED, CAVEAT=SH:CABINET-IN-CONFIDENCE, ACCESS=Personal-Privacy] **PROTECTED//CABINET-IN-CONFIDENCE** **Personal Privacy** This is an example message body. Regards, Rachel
SECRET	X-Protective-Marking: VER=2018.4, NS=2019.2.1.vic.gov.au, SEC=SECRET, ORIGIN=<senderEmailAddress> Subject: This is an example subject line [SEC=SECRET] **SECRET** This is an example message body. Regards, Rachel

Appendix B – Permitted combinations of protective markings

Protective Marking	Caveat		(Optional) Information Management Markers		
	CABINET-IN-CONFIDENCE	NATIONAL CABINET	Legal Privilege	Legislative Secrecy	Personal Privacy
UNOFFICIAL	N	N	N	N	N
OFFICIAL	N	N	N	N	N
OFFICIAL: Sensitive	N	Y	Y[15]	Y[16]	Y[17]
PROTECTED	Y	Y	Y	Y	Y
SECRET	Y	Y	Y	Y	Y

[15] It Is recommended that IMMs only be used in conjuncition with the protective marking of OFFICIAL: Sensitive and above

[16] As above

[17] As above