Preparing for the 2024 Protective Data Security Plan (PDSP)

Victorian Information Security Network (VISN)
February 2024

OVIC
Office of the Victorian
Information Commissioner

We acknowledge the Wurundjeri people of the Kulin Nation as the Traditional Owners of the land from which we are presenting today.

We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.

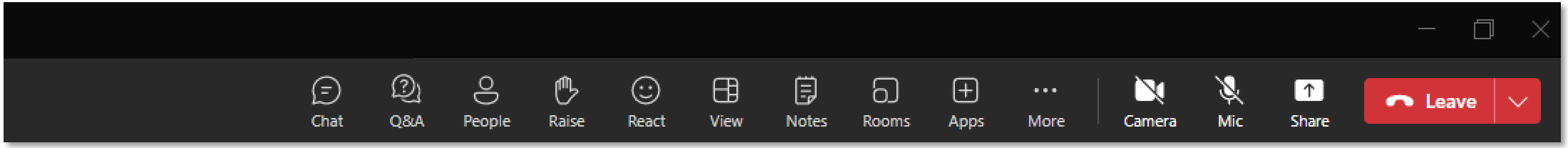
Housekeeping

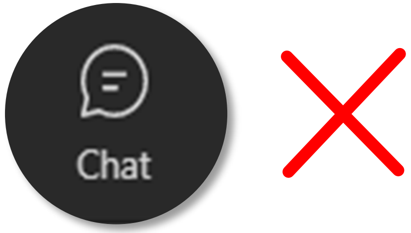
Cameras and mics have been muted for attendees. If your Teams is running slow, try disconnecting from your VPN.

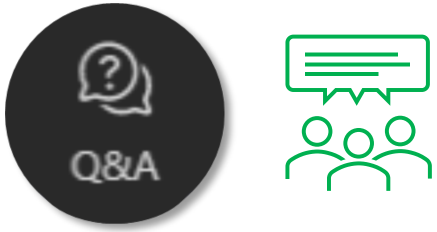
Today's session **is being recorded.**

A copy of OVIC's **slides** and the **recording** will be made available in the coming days on OVIC's website.

Join the conversation







Regular **chat** functionality in Teams has been **disabled** in this forum.

Type your question into the **Teams Q&A channel**.
You can choose to be **anonymous or leave your name displayed**.

Concluding the presentation from ISU, you will have an opportunity to ask questions. If you prefer to ask your question verbally **raise your hand.**

Victorian Information Commissioner

Sean Morrison

Commissioner’s welcome

Sean Morrison

Information Commissioner

- 2024 signals the fourth major reporting cycle for VPS organisations subject to Part 4 of the Privacy and Data Protection Act 2014 (**PDP Act**).
- Letters from Rachel Dixon, Deputy Commissioner, Privacy and Data Protection, outlining this year’s reporting obligations have been sent to public sector body Heads and Information Security Leads.
- Version 3.4 of the PDSP is now available on our website.
- The 2024 PDSP does include some supplementary questions about the use of Artificial Intelligence (**AI**).
- Reminder that the public sector body Head MUST sign the PDSP.
- A range of refreshed resources have been published on the OVIC website to assist your organisation.

Assistant Commissioner – Information Security

Anthony Corso

Agenda

- Purpose of today’s session and updates to OVIC website
- Re-cap on legislative obligations
- What’s changed on the 2024 Protective Data Security Plan (**PDSP**) form
- Preparing for the 2024 PDSP
- Questions
- Deputy Commissioner - What’s next and final thoughts

Purpose of today’s session

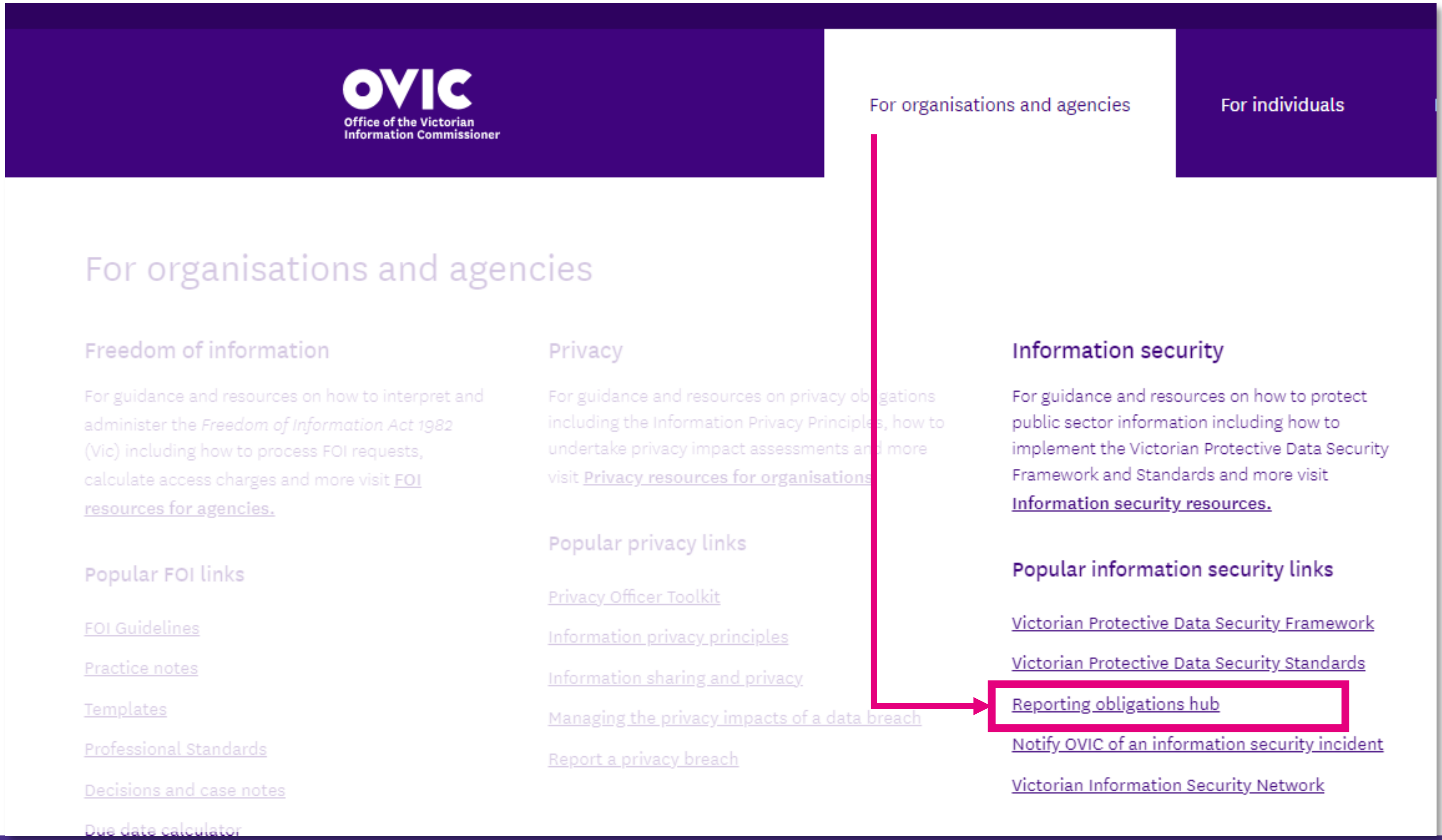
- This presentation is geared towards those who have previously reported.
- This session won’t provide step by step guidance on how to approach this process.

- For those who are new to this process, ensure you take a look at the resources on our website.
- Review the *2024 - How to: A Guide to completing a PDSP.*
- We are considering some additional resources to offer further assistance.
- If after reviewing these resources, and you require further help, reach out to security@ovic.vic.gov.au

  One of our Senior Business Engagement Officers will be in touch.

Updates to the website – VPS stakeholders

The Information Security section of OVIC's website has been refreshed with content for the 2024 reporting cycle



OVIC
Office of the Victorian
Information Commissioner

For organisations and agencies

For individuals

For organisations and agencies

Freedom of information

For guidance and resources on how to interpret and administer the *Freedom of Information Act 1982* (Vic) including how to process FOI requests, calculate access charges and more visit FOI resources for agencies.

Popular FOI links

- FOI Guidelines
- Practice notes
- Templates
- Professional Standards
- Decisions and case notes
- Due date calculator

Privacy

For guidance and resources on privacy obligations including the Information Privacy Principles, how to undertake privacy impact assessments and more visit **Privacy resources for organisations**

Popular privacy links

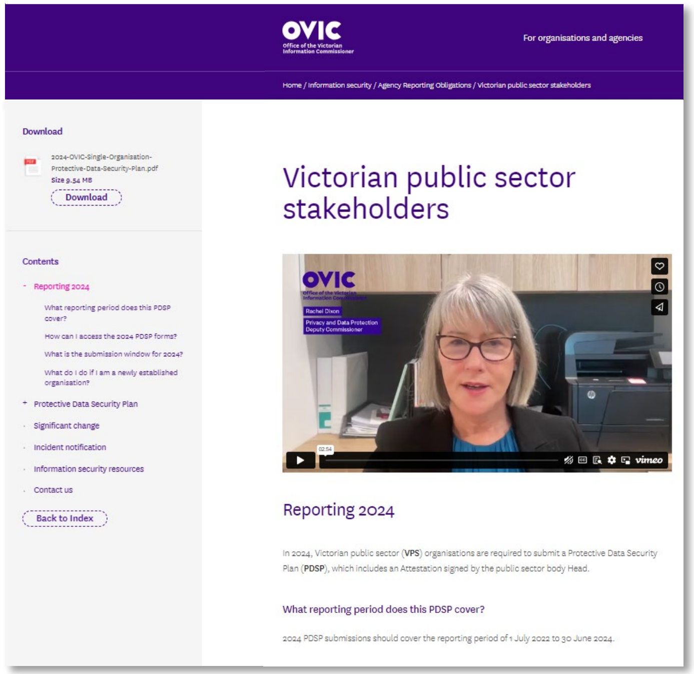
- Privacy Officer Toolkit
- Information privacy principles
- Information sharing and privacy
- Managing the privacy impacts of a data breach
- Report a privacy breach

Information security

For guidance and resources on how to protect public sector information including how to implement the Victorian Protective Data Security Framework and Standards and more visit **Information security resources.**

Popular information security links

- Victorian Protective Data Security Framework
- Victorian Protective Data Security Standards
- Reporting obligations hub
- Notify OVIC of an information security incident
- Victorian Information Security Network



OVIC
Office of the Victorian
Information Commissioner

For organisations and agencies

Home / Information security / Agency Reporting Obligations / Victorian public sector stakeholders

Download

2024-OVIC-Single-Organisation-Protective-Data-Security-Plan.pdf
Size 9.54 MB

Download

Contents

- Reporting 2024
  - What reporting period does this PDSP cover?
  - How can I access the 2024 PDSP forms?
  - What is the submission window for 2024?
  - What do I do if I am a newly established organisation?
- Protective Data Security Plan
- Significant change
- Incident notification
- Information security resources
- Contact us

Back to Index

Victorian public sector stakeholders

OVIC
Office of the Victorian Information Commissioner
Rachel Dixon
Privacy and Data Protection Deputy Commissioner
02:54
vimeo

Reporting 2024

In 2024, Victorian public sector (**VPS**) organisations are required to submit a Protective Data Security Plan (**PDSP**), which includes an Attestation signed by the public sector body Head.

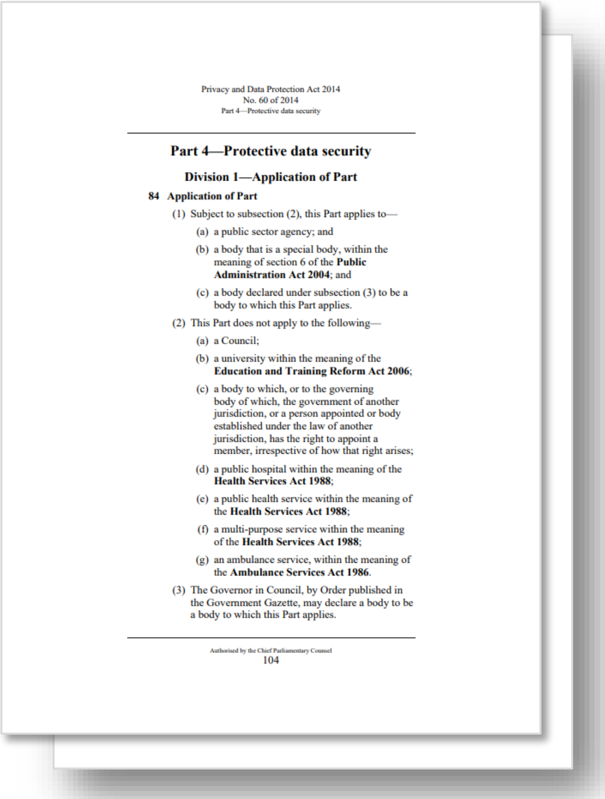
What reporting period does this PDSP cover?

2024 PDSP submissions should cover the reporting period of 1 July 2022 to 30 June 2024.

Legislative Obligations

Office of the Victorian
Information Commissioner

Part 4 of the PDP Act



Privacy and Data Protection Act 2014
No. 60 of 2014
Part 4—Protective data security

Part 4—Protective data security

Division 1—Application of Part

84 Application of Part

(1) Subject to subsection (2), this Part applies to—

(a) a public sector agency; and

(b) a body that is a special body, within the meaning of section 6 of the **Public Administration Act 2004**; and

(c) a body declared under subsection (3) to be a body to which this Part applies.

(2) This Part does not apply to the following—

(a) a Council;

(b) a university within the meaning of the **Education and Training Reform Act 2006**;

(c) a body to which, or to the governing body of which, the government of another jurisdiction, or a person appointed or body established under the law of another jurisdiction, has the right to appoint a member, irrespective of how that right arises;

(d) a public hospital within the meaning of the **Health Services Act 1988**;

(e) a public health service within the meaning of the **Health Services Act 1988**;

(f) a multi-purpose service within the meaning of the **Health Services Act 1988**;

(g) an ambulance service, within the meaning of the **Ambulance Services Act 1986**.

(3) The Governor in Council, by Order published in the Government Gazette, may declare a body to be a body to which this Part applies.

Authorised by the Chief Parliamentary Counsel
104

Security Risk Profile Assessment

(SRPA)

Section 89(1)(a) The public sector body Head must ensure that a security risk profile assessment is undertaken for the agency or body

Section 89(2) A security risk profile assessment of an agency or body **must include an assessment of any contracted service provider** of the agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body.

Protective Data Security Plan

(PDSP)

Section 89(4) A public sector body Head must ensure that the protective data security plan prepared under this section is reviewed--

(a) if there is a **significant change** in the operating environment or the security risks relevant to the agency or body; or

(b) otherwise, **every 2 years**.

Section 89(5) A public sector body Head for the agency or body must ensure that a copy of the protective data security plan is given to the Information Commissioner.

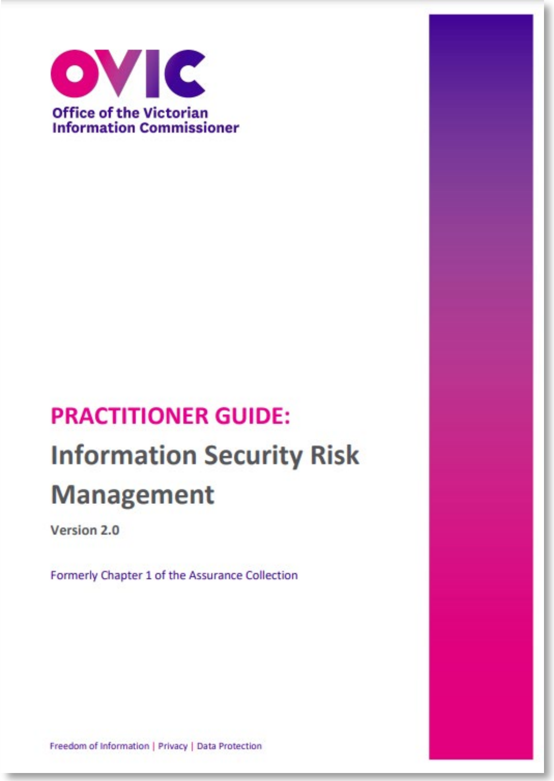
Security Risk Profile Assessment (SRPA) process

A Security Risk Profile Assessment (**SRPA**) is a powerful **process** for identifying and prioritising information security risks and controls.

This process includes an assessment of the risks of information assets across all security domains - **information** security, **physical** security, **personnel** security; and **ICT** security.

Remember: The SRPA refers to a process, not a product!

Refer to your organisations existing risk management framework



OVIC
Office of the Victorian
Information Commissioner

PRACTITIONER GUIDE:

Information Security Risk Management

Version 2.0

Formerly Chapter 1 of the Assurance Collection

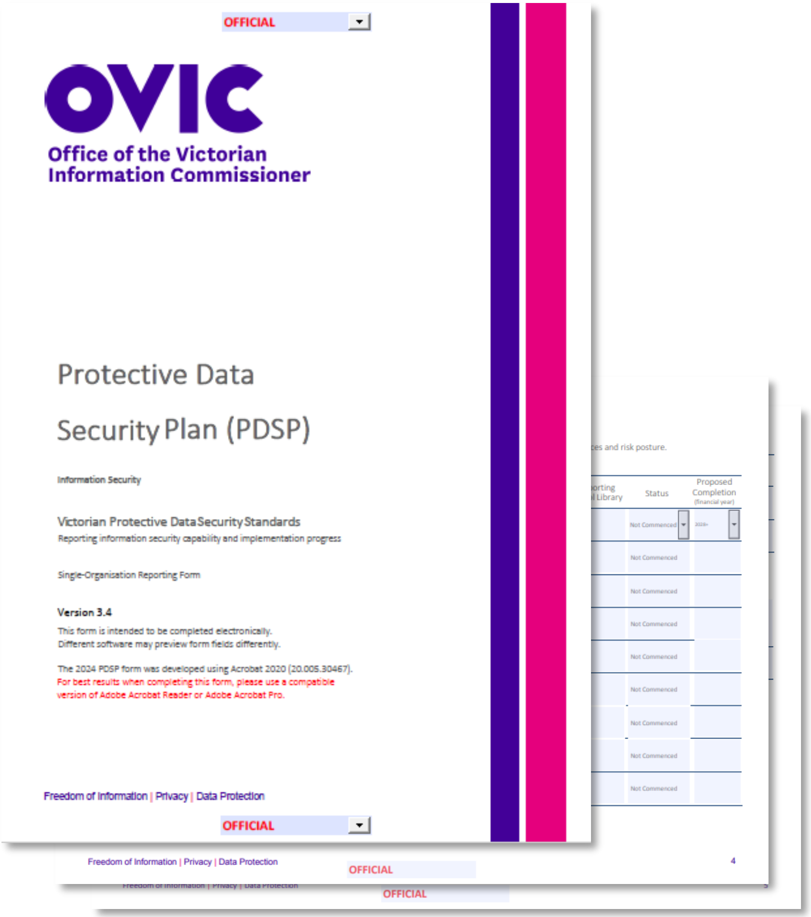
Freedom of Information | Privacy | Data Protection

For more info on how to conduct the SRPA process navigate to -

https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/

What’s changed on the 2024 PDSP?

New 2024 PDSP form (V3.4)



OFFICIAL

OVIC
Office of the Victorian
Information Commissioner

Protective Data

Security Plan (PDSP)

Information Security

Victorian Protective Data Security Standards
Reporting information security capability and implementation progress

Single-Organisation Reporting Form

Version 3.4

This form is intended to be completed electronically.
Different software may preview form fields differently.

The 2024 PDSP form was developed using Acrobat 2020 (20.005.30467).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

...es and risk posture.

...orting ...l Library	Status	Proposed Completion (financial year)
	Not Commenced	2028-
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	

Freedom of Information | Privacy | Data Protection

OFFICIAL

4

Freedom of Information | Privacy | Data Protection

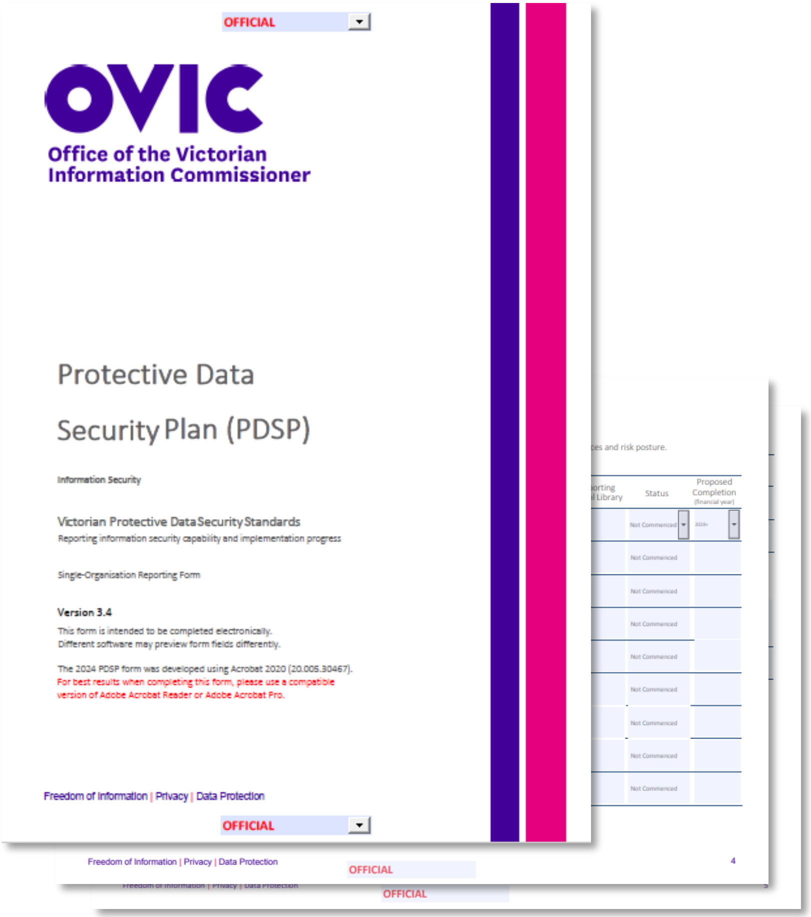
OFFICIAL

5

Ensure you are using the most current version of the 2024 PDSP template!

- A copy of the 2024 Protective Data Security Plan (PDSP) was released last week, however this has since been updated.
- If you have accessed this form before 26 February 2024, ensure you download and use the **updated version 3.4.**
- The new version (V3.4) of the form is now available on the OVIC website.
- If you have any questions, email security@ovic.vic.gov.au

New 2024 PDSP form (V3.4) - continued



OFFICIAL

Office of the Victorian Information Commissioner

Protective Data Security Plan (PDSP)

Information Security

Victorian Protective Data Security Standards
Reporting information security capability and implementation progress

Single-Organisation Reporting Form

Version 3.4

This form is intended to be completed electronically.
Different software may preview form fields differently.

The 2024 PDSP form was developed using Acrobat 2020 (20.005.30467).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

ces and risk posture.

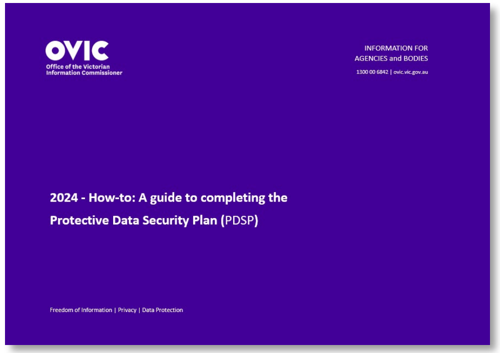
orting l Library	Status	Proposed Completion (financial year)
	Not Commenced	2026+
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	

Freedom of Information | Privacy | Data Protection OFFICIAL 4

Download a copy of the **2024 PDSP form**:

https://go.vic.gov.au/3SV58pv

Download a copy of the **2024 - How to: A guide to completing the Protective Data Security Plan (PDSP)**



Office of the Victorian Information Commissioner

INFORMATION FOR
AGENCIES and BODIES
1300 00 6842 | ovic.vic.gov.au

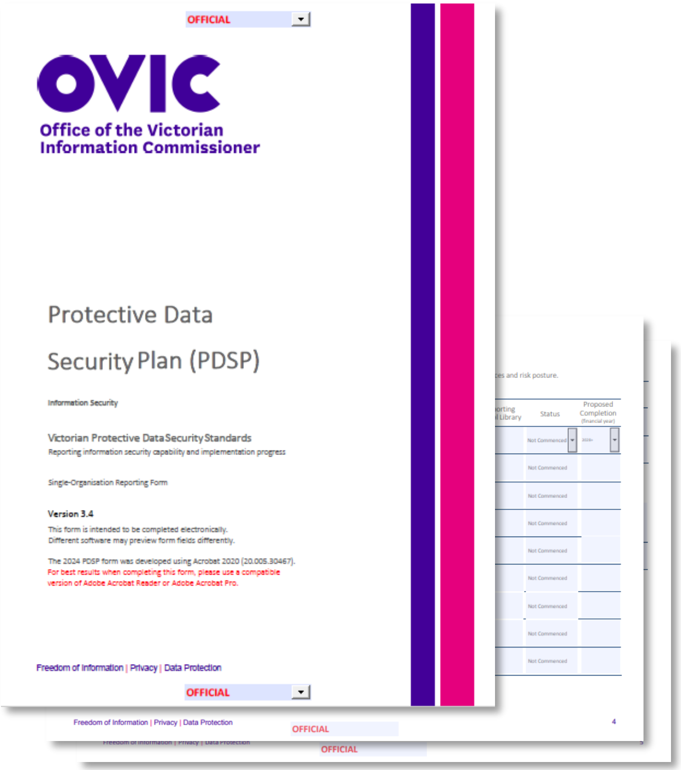
2024 - How-to: A guide to completing the Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

https://go.vic.gov.au/48xC656

Contains FAQs and helpful instructions on completing the PDSP form.

What’s changed on the 2024 PDSP form?



OFFICIAL

OVIC
Office of the Victorian
Information Commissioner

Protective Data

Security Plan (PDSP)

Information Security

Victorian Protective Data Security Standards
Reporting information security capability and implementation progress

Single-Organisation Reporting Form

Version 3.4

This form is intended to be completed electronically.
Different software may preview form fields differently.

The 2024 PDSP form was developed using Acrobat 2020 (20.005.30467).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

…es and risk posture.

…orting …l Library	Status	Proposed Completion (financial year)
	Not Commenced	2024+
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	

Freedom of Information | Privacy | Data Protection OFFICIAL 4

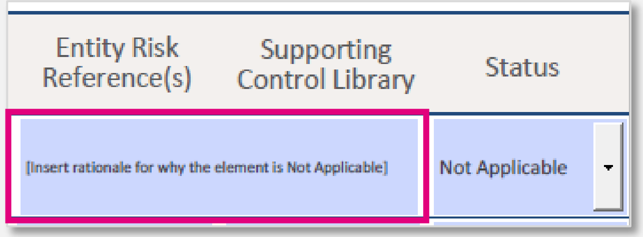
Freedom of Information | Privacy | Data Protection OFFICIAL

- JavaScript has been removed resulting in loss of automated functions within the form
- The FAQ section has been removed and incorporated into the 2024 How to Guide
- Adjusted the use of the commentary box at the end of each Standard, allowing users to add mandatory and/or supplementary content or narratives
- Industrial Automation and Control Systems (IACS) elements have been added to VPDSS 1 and 2
- Standard 9 elements and accompanying responses have been incorporated of into Attestation section of the PDSP form
- Changes to Organisation Profile Assessment (OPA):
  - removal of JavaScript resulting in information asset percentages not automatically calculating
  - added Artificial Intelligence (AI) usage / uptake-based questions
- Attestation wording has been amended
- Refreshed options for inserting a signature in the Attestation

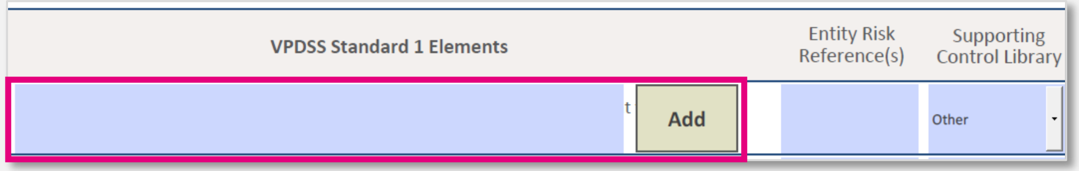
Javascript removed

Former form

In previous iterations of the PDSP form, JavaScript was used to offer automated functionality for certain fields. (examples shown below)



Entity Risk Reference(s)	Supporting Control Library	Status
[Insert rationale for why the element is Not Applicable]		Not Applicable



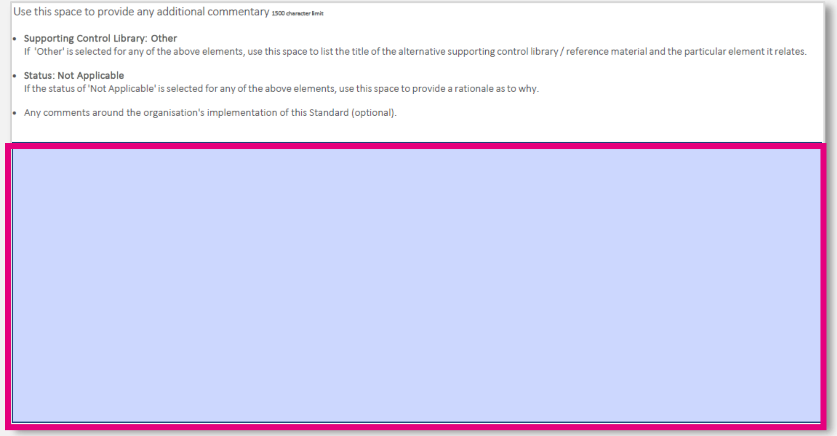
VPDSS Standard 1 Elements	Entity Risk Reference(s)	Supporting Control Library
Add		Other

This automated functionality has been removed.

Current form

To cater for this removal, OVIC has adjusted the way the **commentary box** at the end of each Standard is used.

Use this box to provide additional *mandatory* content and/or *supplementary* commentary in support of the Standard.

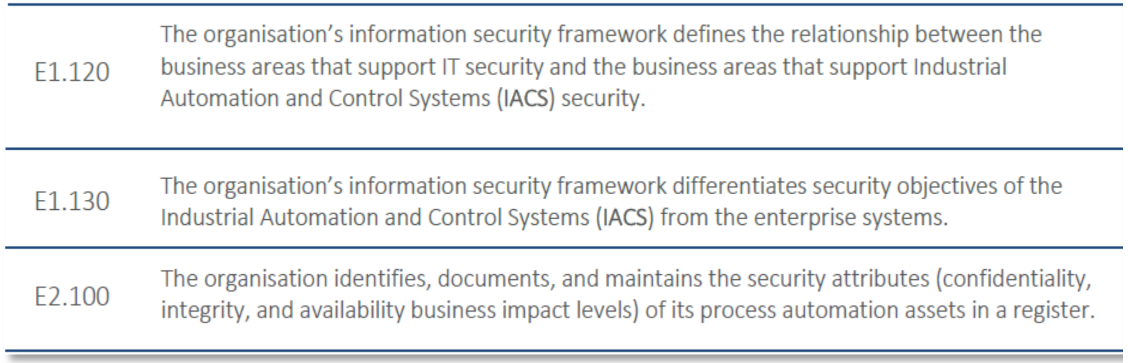


Use this space to provide any additional commentary 1500 character limit

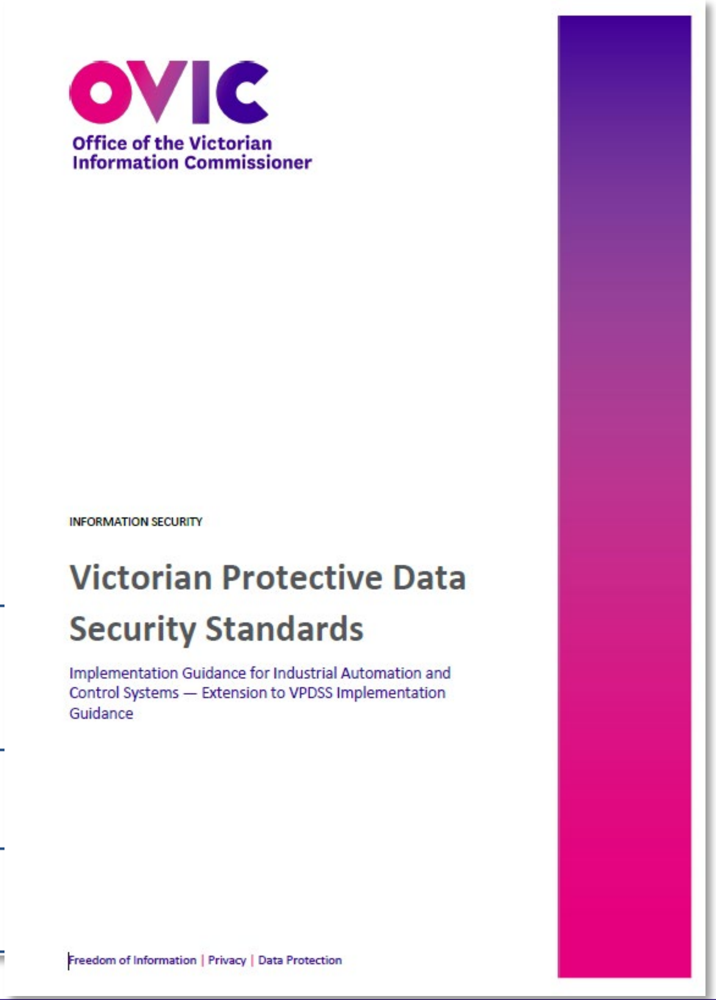
- **Supporting Control Library: Other**
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- **Status: Not Applicable**
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Industrial Automation and Control Systems (IACS) elements

- **Three new elements** have been included in the 2024 PDSP for Standard 1 and 2.
- These elements only to those organisations that operate IACS.
- If these elements do not apply to your environment, select *Not Applicable* for E1.120, E1.130 and E2.100 on the PDSP form.
- For further guidance on these specific elements, refer to the *IACS –Extension to the VPDSS Implementation Guidance (V1.0).*



E1.120	The organisation's information security framework defines the relationship between the business areas that support IT security and the business areas that support Industrial Automation and Control Systems (IACS) security.
E1.130	The organisation's information security framework differentiates security objectives of the Industrial Automation and Control Systems (IACS) from the enterprise systems.
E2.100	The organisation identifies, documents, and maintains the security attributes (confidentiality, integrity, and availability business impact levels) of its process automation assets in a register.



OVIC
Office of the Victorian
Information Commissioner

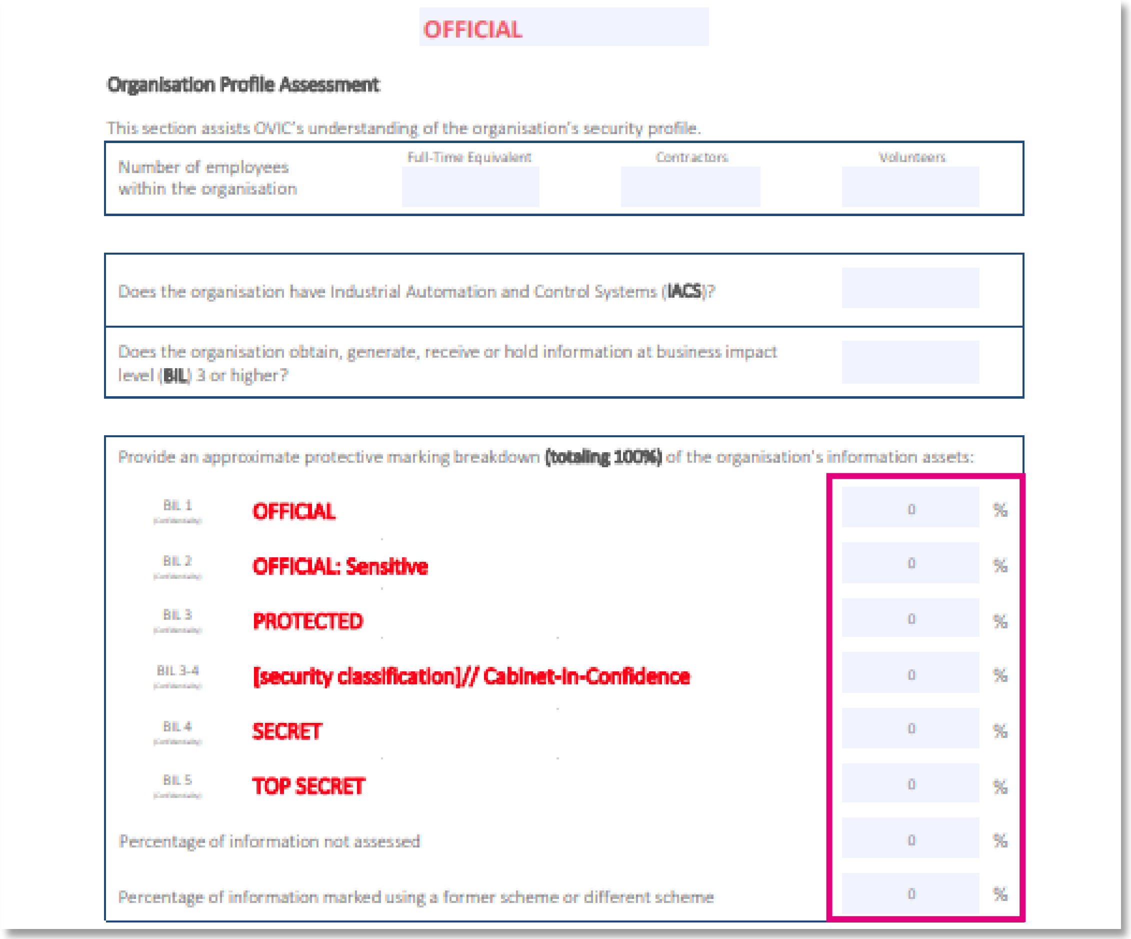
INFORMATION SECURITY

Victorian Protective Data Security Standards

Implementation Guidance for Industrial Automation and Control Systems — Extension to VPDSS Implementation Guidance

Freedom of Information | Privacy | Data Protection

OPA - Removal of automated calculation feature



OFFICIAL

Organisation Profile Assessment

This section assists OVIC's understanding of the organisation's security profile.

	Full-Time Equivalent	Contractors	Volunteers
Number of employees within the organisation			

Does the organisation have Industrial Automation and Control Systems (**IACS**)?	
Does the organisation obtain, generate, receive or hold information at business impact level (**BIL**) 3 or higher?	

Provide an approximate protective marking breakdown **(totaling 100%)** of the organisation's information assets:

BIL 1 (Confidentiality)	OFFICIAL	0	%
BIL 2 (Confidentiality)	OFFICIAL: Sensitive	0	%
BIL 3 (Confidentiality)	PROTECTED	0	%
BIL 3-4 (Confidentiality)	[security classification]// Cabinet-In-Confidence	0	%
BIL 4 (Confidentiality)	SECRET	0	%
BIL 5 (Confidentiality)	TOP SECRET	0	%
Percentage of information not assessed		0	%
Percentage of information marked using a former scheme or different scheme		0	%

- This section includes several mandatory questions to provide insight into the broader profile of your organisation.
- Whilst most fields in this section remain unchanged, the removal of Javascript has resulted in the **removal of an automated calculation feature.**
- As such, users will need to **manually calculate** an **approximate protective marking breakdown for information asset percentages**, ensuring they come to a **total of 100%.**

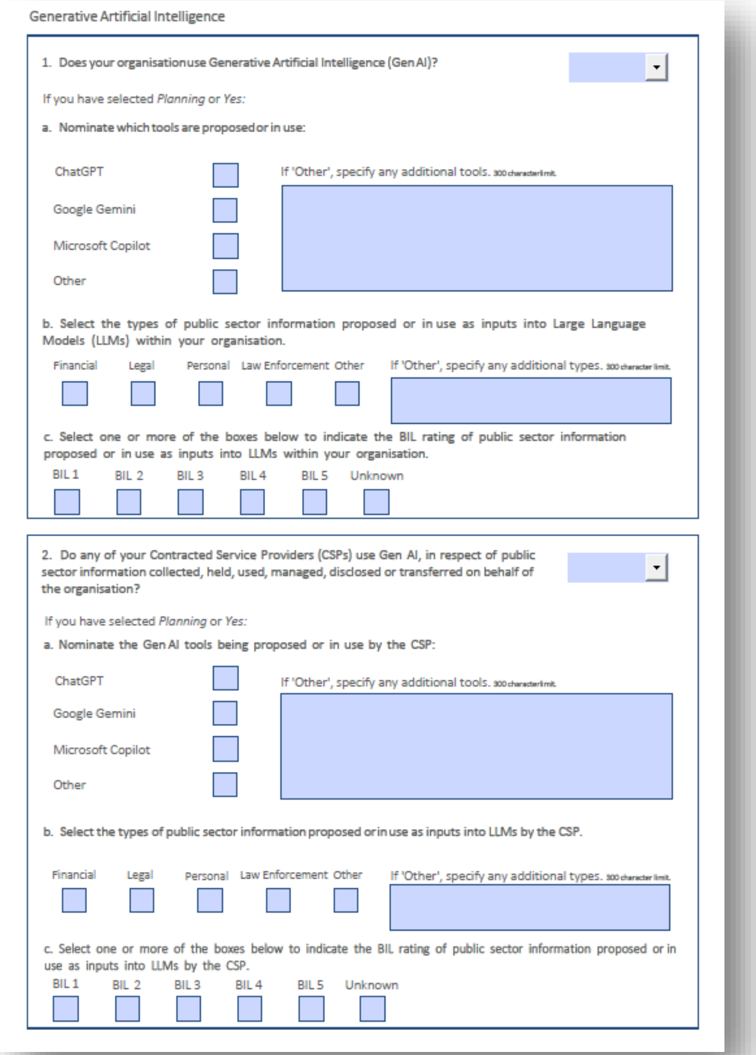
OPA – Supplementary Artificial Intelligence (AI) questionnaire

- Supplementary Artificial Intelligence (**AI**) questions have been introduced this year into the OPA section of the PDSP.

  This is based on an uptake in proposals and questions surrounding the use and integration of AI tools and services.

- As such, your organisation **MUST use V3.4 of the 2024 PDSP form** which has been uploaded to the OVIC website just this week. This replaces all former versions of the form.

- If you accessed an earlier version of the 2024 PDSP form in the last week or so, please download and use this updated version (V3.4).



Generative Artificial Intelligence

1. Does your organisationuse Generative Artificial Intelligence (Gen AI)? ▾

If you have selected Planning or Yes:

a. Nominate which tools are proposedor in use:

ChatGPT □
Google Gemini □
Microsoft Copilot □
Other □

If 'Other', specify any additional tools. 300 character limit.

b. Select the types of public sector information proposed or in use as inputs into Large Language Models (LLMs) within your organisation.

Financial	Legal	Personal	Law Enforcement	Other
□	□	□	□	□

If 'Other', specify any additional types. 300 character limit.

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs within your organisation.

BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	Unknown
□	□	□	□	□	□

2. Do any of your Contracted Service Providers (CSPs) use Gen AI, in respect of public sector information collected, held, used, managed, disclosed or transferred on behalf of the organisation? ▾

If you have selected Planning or Yes:

a. Nominate the Gen AI tools being proposed or in use by the CSP:

ChatGPT □
Google Gemini □
Microsoft Copilot □
Other □

If 'Other', specify any additional tools. 300 character limit.

b. Select the types of public sector information proposed or in use as inputs into LLMs by the CSP.

Financial	Legal	Personal	Law Enforcement	Other
□	□	□	□	□

If 'Other', specify any additional types. 300 character limit.

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs by the CSP.

BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	Unknown
□	□	□	□	□	□

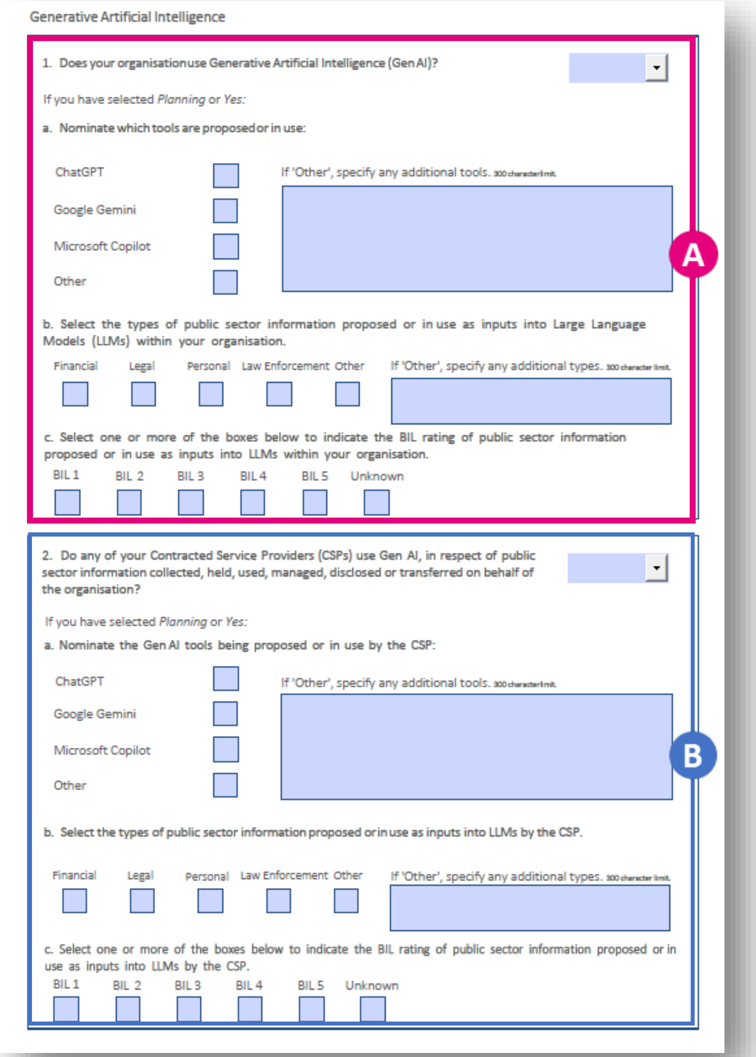
OPA – Supplementary AI questionnaire (continued)

- There are two broad sets of questions in this section –

A	Does your organisation use Generative AI (**Gen AI**)?
B	Do contracted service providers (**CSPs**) use Gen AI in respect of public sector information collected, held, managed, disclosed or transferred on behalf of the organisation?

- The form offers the following selections as a drop-down response -
  - *Unsure*
  - *No*
  - *Planning*
  - *Yes*

- If you select *Planning* or *Yes*, subsequent questions must be answered regarding the:
  - Gen AI tool;
  - types of information proposed or in use as an input; and
  - security value of this information.



Generative Artificial Intelligence

1. Does your organisationuse Generative Artificial Intelligence (Gen AI)? ▾

If you have selected *Planning* or *Yes:*

a. Nominate which tools are proposedor in use:

ChatGPT □
Google Gemini □
Microsoft Copilot □
Other □

If 'Other', specify any additional tools. 300 character limit.

b. Select the types of public sector information proposed or in use as inputs into Large Language Models (LLMs) within your organisation.

Financial □ Legal □ Personal □ Law Enforcement □ Other □

If 'Other', specify any additional types. 300 character limit.

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs within your organisation.

BIL 1 □ BIL 2 □ BIL 3 □ BIL 4 □ BIL 5 □ Unknown □

2. Do any of your Contracted Service Providers (CSPs) use Gen AI, in respect of public sector information collected, held, used, managed, disclosed or transferred on behalf of the organisation? ▾

If you have selected *Planning* or *Yes:*

a. Nominate the Gen AI tools being proposed or in use by the CSP:

ChatGPT □
Google Gemini □
Microsoft Copilot □
Other □

If 'Other', specify any additional tools. 300 character limit.

b. Select the types of public sector information proposed orin use as inputs into LLMs by the CSP.

Financial □ Legal □ Personal □ Law Enforcement □ Other □

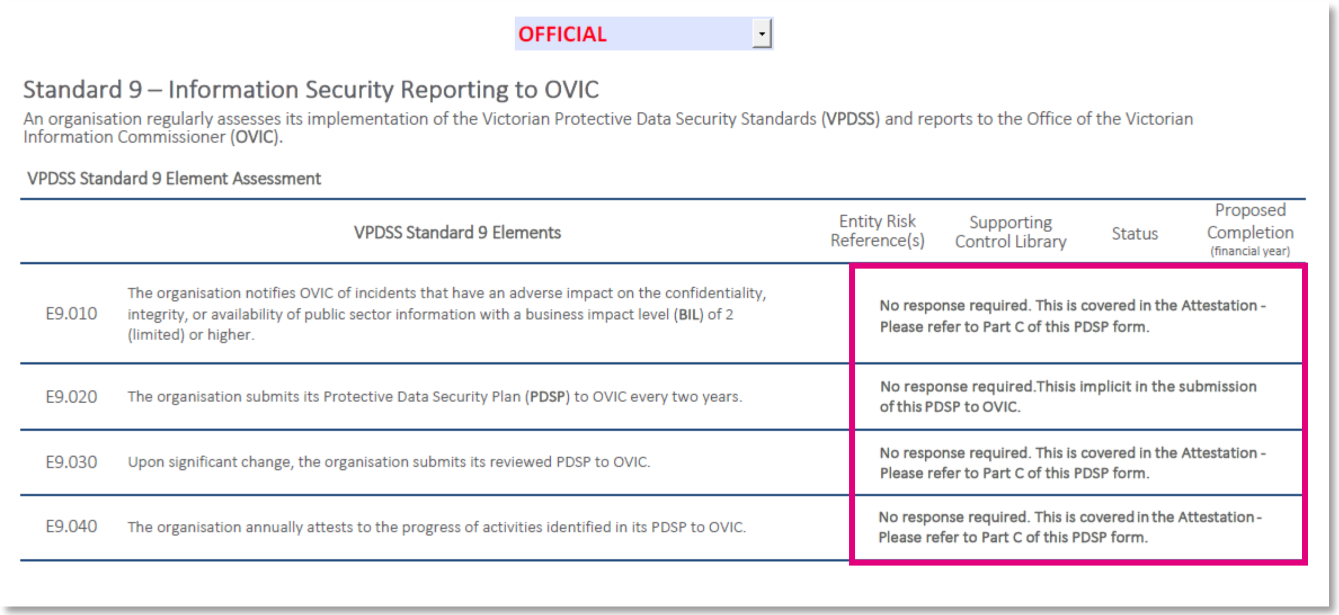
If 'Other', specify any additional types. 300 character limit.

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs by the CSP.

BIL 1 □ BIL 2 □ BIL 3 □ BIL 4 □ BIL 5 □ Unknown □

Standard 9 elements

Feedback from previous reporting cycles noted confusion on how to respond to the Standard 9 elements.



OFFICIAL

Standard 9 – Information Security Reporting to OVIC

An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (**VPDSS**) and reports to the Office of the Victorian Information Commissioner (**OVIC**).

VPDSS Standard 9 Element Assessment

	VPDSS Standard 9 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E9.010	The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level (**BIL**) of 2 (limited) or higher.	No response required. This is covered in the Attestation - Please refer to Part C of this PDSP form.			
E9.020	The organisation submits its Protective Data Security Plan (**PDSP**) to OVIC every two years.	No response required.Thisis implicit in the submission of this PDSP to OVIC.			
E9.030	Upon significant change, the organisation submits its reviewed PDSP to OVIC.	No response required. This is covered in the Attestation - Please refer to Part C of this PDSP form.			
E9.040	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.	No response required. This is covered in the Attestation - Please refer to Part C of this PDSP form.			

In response, **Standard 9 elements have been incorporated into the Attestation** by the public sector body Head.

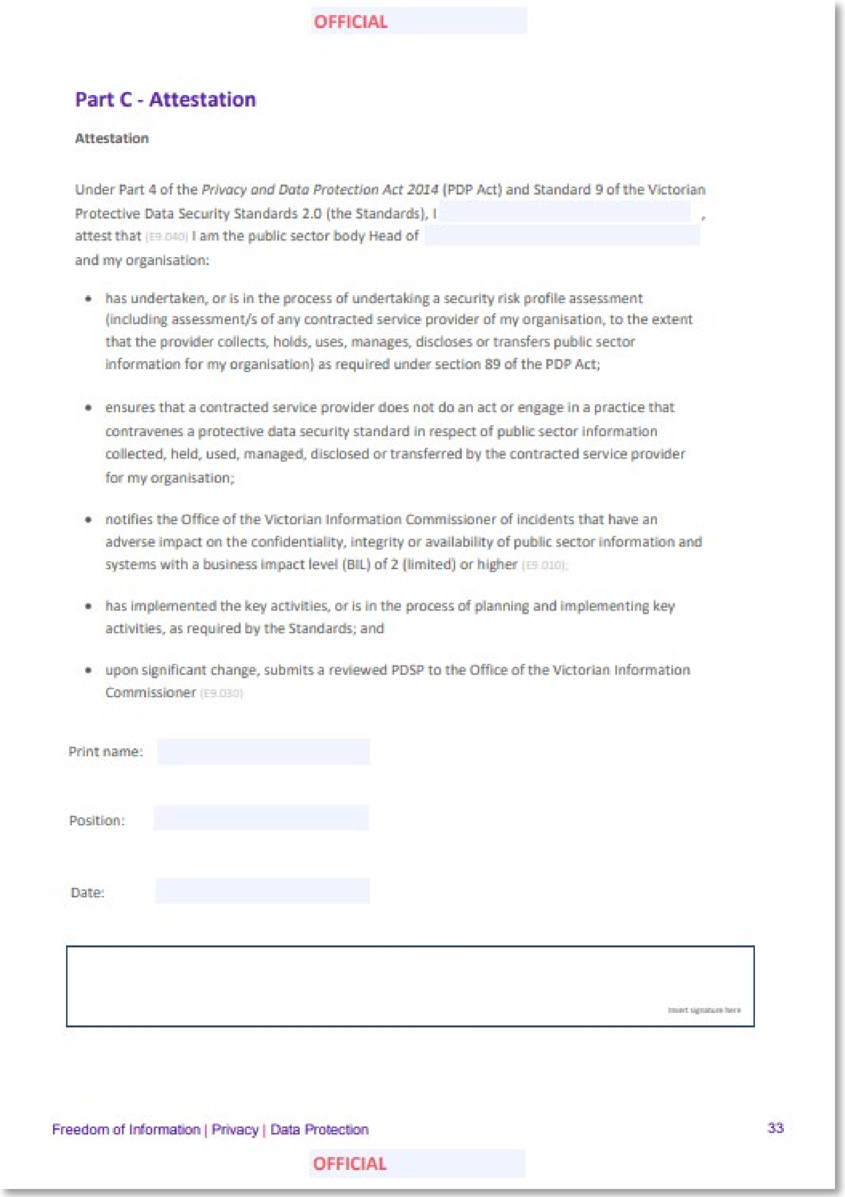
As such, responses are not required for Standard 9, found on page 22 of the PDSP form.

Attestation

The purpose of the Attestation is to **confirm/reaffirm** that the organisation is **continuing its program of security activities to address the VPDSS as outlined in the PDSP**, including confirmation that the organisation has undertaken the SRPA process.

- The annual submission of an Attestation to OVIC is a requirement under element E9.040.

- In acknowledgement of their obligations under Part 4 of PDP Act, the Attestation **must be signed by the public sector body Head** and cannot be delegated to another person.



OFFICIAL

Part C - Attestation

Attestation

Under Part 4 of the *Privacy and Data Protection Act 2014* (PDP Act) and Standard 9 of the Victorian Protective Data Security Standards 2.0 (the Standards), I ,
attest that (E9.040) I am the public sector body Head of
and my organisation:

- has undertaken, or is in the process of undertaking a security risk profile assessment (including assessment/s of any contracted service provider of my organisation, to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector information for my organisation) as required under section 89 of the PDP Act;
- ensures that a contracted service provider does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector information collected, held, used, managed, disclosed or transferred by the contracted service provider for my organisation;
- notifies the Office of the Victorian Information Commissioner of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information and systems with a business impact level (BIL) of 2 (limited) or higher (E9.010);
- has implemented the key activities, or is in the process of planning and implementing key activities, as required by the Standards; and
- upon significant change, submits a reviewed PDSP to the Office of the Victorian Information Commissioner (E9.030)

Print name:

Position:

Date:

Insert signature here

Freedom of Information | Privacy | Data Protection 33

OFFICIAL

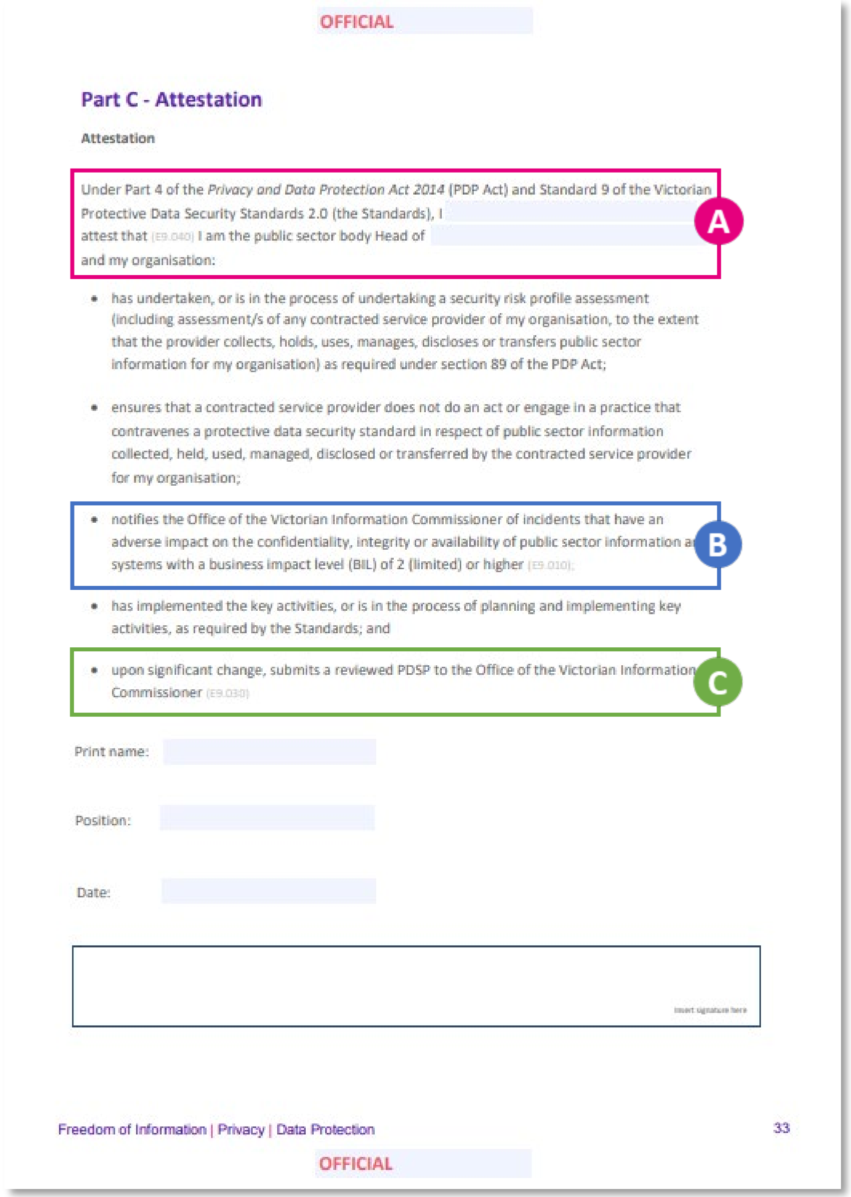
Updates to the Attestation in 2024

In 2024, the Attestation wording has been enhanced. This includes the incorporation of three elements from Standard 9.

Image Ref.	Element	Description
A	E9.040	These elements are covered in the Attestation. No response required for these elements on page 22 of the PDSP form.
B	E9.010	
C	E9.030	

E9.020 This element is satisfied via the submission of a current copy of the PDSP form to OVIC.

No further response is required for this element (either on page 22 of the PDSP form or in the Attestation itself).



OFFICIAL

Part C - Attestation

Attestation

Under Part 4 of the *Privacy and Data Protection Act 2014* (PDP Act) and Standard 9 of the Victorian Protective Data Security Standards 2.0 (the Standards), I attest that (E9.040) I am the public sector body Head of and my organisation:

- has undertaken, or is in the process of undertaking a security risk profile assessment (including assessment/s of any contracted service provider of my organisation, to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector information for my organisation) as required under section 89 of the PDP Act;
- ensures that a contracted service provider does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector information collected, held, used, managed, disclosed or transferred by the contracted service provider for my organisation;
- notifies the Office of the Victorian Information Commissioner of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information a systems with a business impact level (BIL) of 2 (limited) or higher (E9.010);
- has implemented the key activities, or is in the process of planning and implementing key activities, as required by the Standards; and
- upon significant change, submits a reviewed PDSP to the Office of the Victorian Information Commissioner (E9.030)

Print name:

Position:

Date:

Insert signature here

Freedom of Information | Privacy | Data Protection 33

OFFICIAL

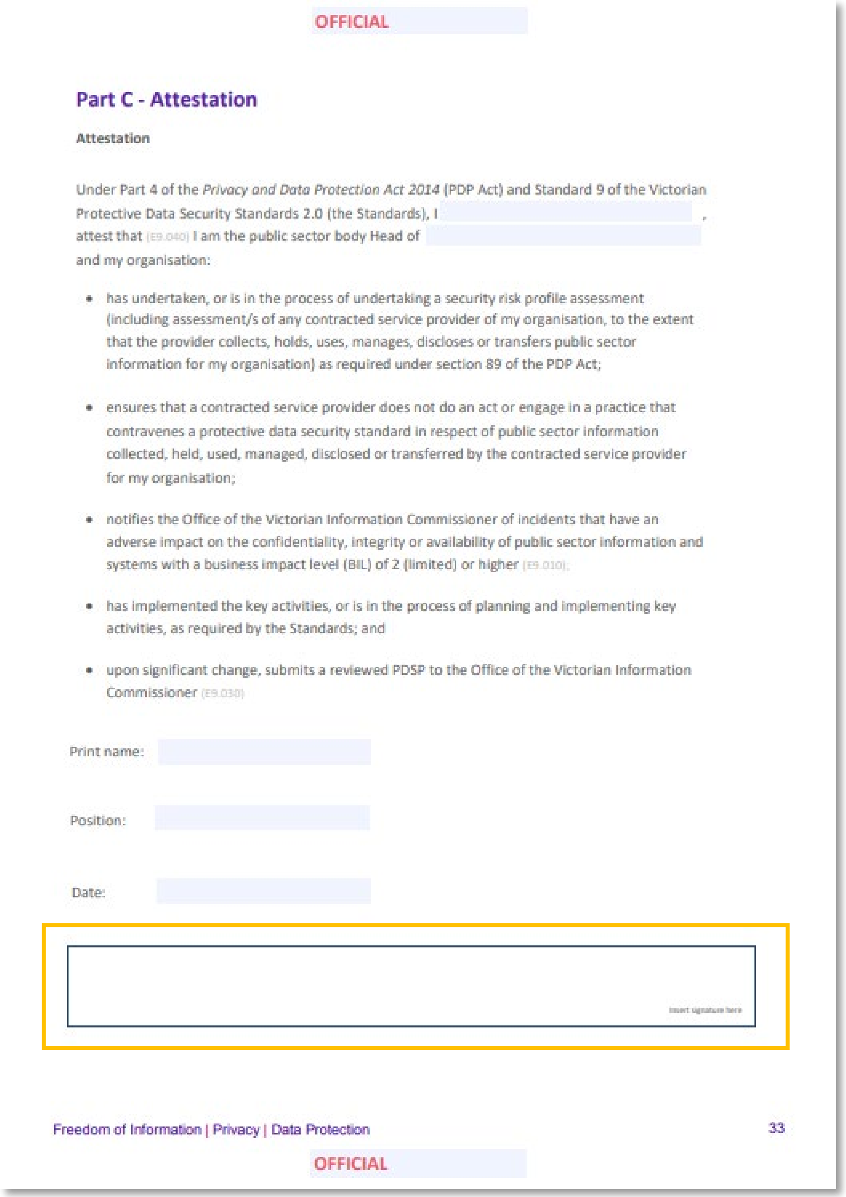
Signing the 2024 Attestation

Soft copy / electronic signing

Option 1	Use the Adobe **Acrobat Reader Fill & Sign feature** to add the public sector body Head's signature into the box provided on the Attestation.
Option 2	**Insert an image file** (e.g. jpg, tiff, bmp) of the public sector body Head's signature into the box provided on the Attestation.
Option 3	**Type the name** of the public sector body Head's signature into the box provided on the Attestation.

Hard copy signing

Option 4	Print a hard copy of the completed PDSP for the public sector body Head to **physically review, sign and date with a wet signature**. This signed and dated hard copy Attestation may be scanned and combined with the remainder of the PDSP.



OFFICIAL

Part C - Attestation

Attestation

Under Part 4 of the *Privacy and Data Protection Act 2014* (PDP Act) and Standard 9 of the Victorian Protective Data Security Standards 2.0 (the Standards), I ,
attest that (E9.040) I am the public sector body Head of
and my organisation:

- has undertaken, or is in the process of undertaking a security risk profile assessment (including assessment/s of any contracted service provider of my organisation, to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector information for my organisation) as required under section 89 of the PDP Act;
- ensures that a contracted service provider does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector information collected, held, used, managed, disclosed or transferred by the contracted service provider for my organisation;
- notifies the Office of the Victorian Information Commissioner of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information and systems with a business impact level (BIL) of 2 (limited) or higher (E9.010);
- has implemented the key activities, or is in the process of planning and implementing key activities, as required by the Standards; and
- upon significant change, submits a reviewed PDSP to the Office of the Victorian Information Commissioner (E9.030)

Print name:

Position:

Date:

Insert signature here

Freedom of Information | Privacy | Data Protection 33

OFFICIAL

Preparing for the 2024 PDSP

Suggested process

1 Engage the public sector body Head

- **Accountability of the PDSP** sits with the public sector body Head
  - Make sure to involve them throughout the year so they are comfortable in signing the Attestation
  - Advise them of the timeline / approach for reporting by **August 31, 2024**

2 Engage your VPDSS working group

- This group may be made up of representatives (internal and external) from -
  - Governance
  - Legal
  - People and Culture
  - Facilities
  - Risk/Internal Audit
  - Finance
  - ICT
  - Information/Records Management
  - Contracted Service Providers
  - Portfolio Department
    (especially where they provide services, support or infrastructure)

3 Review your previous PDSP

- Contact security@ovic.vic.gov.au if you can't locate a copy

Suggested process (continued)

4 Conduct an updated review of information security risks and treatments

- This process may include a review of the organisations previous PDSP, risk register, Information Asset Register (including security value assessments), incident register, treatment plans, as well as consideration of any Contracted Service Providers risks
- By completing this review, you are meeting your legislative obligations of undertaking the **SRPA process**

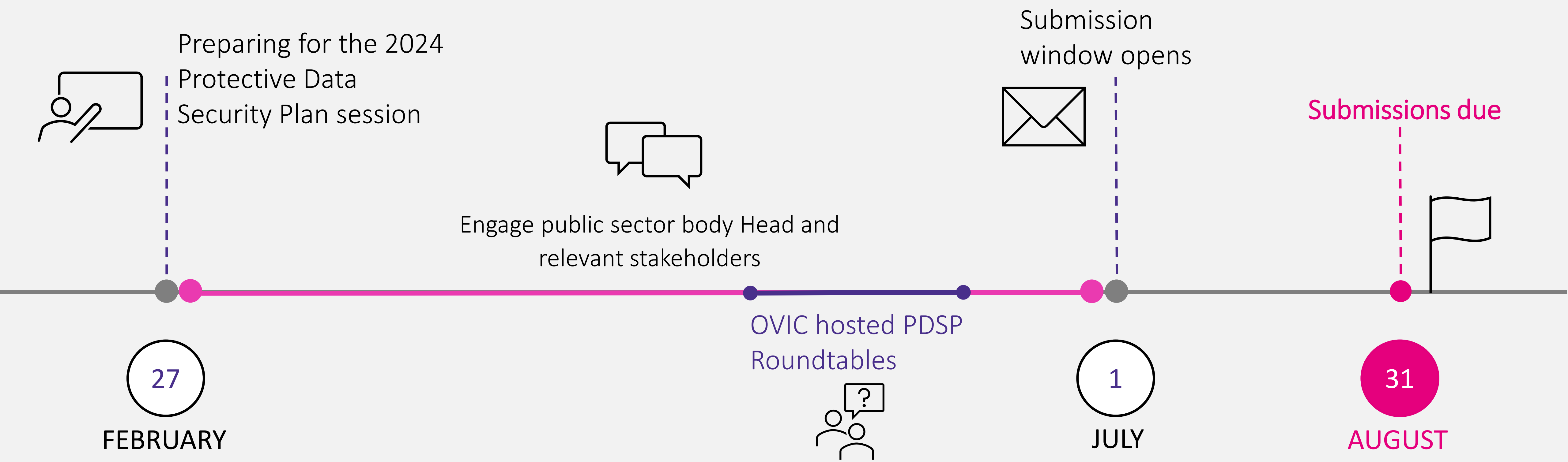
5 Enter responses into the 2024 PDSP form

- Ensure you are using updated 2024 PDSP form (V3.4)

6 Attestation signed by public sector body Head

- Brief your public sector body Head and have them review the PDSP and sign the Attestation
  - *Consider any internal processing time, to allow enough opportunity to gain sign off and submission by 31 August 2024.*

When? PDSP reporting timeline

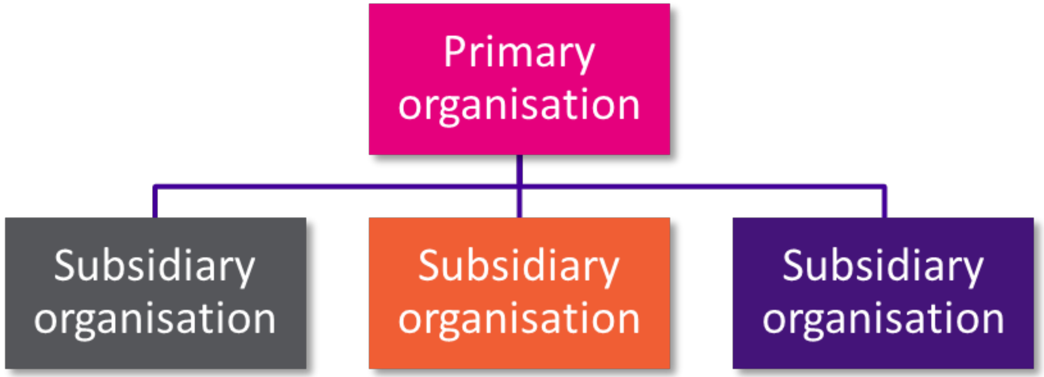


Preparing for the 2024 Protective Data Security Plan session
Engage public sector body Head and relevant stakeholders
Submission window opens
Submissions due
OVIC hosted PDSP Roundtables
?
27
FEBRUARY
1
JULY
31
AUGUST

Ensure you consider internal processes to allow enough time to gain sign off

2024 Multi-Organisation reporting model

- OVIC is aware that some organisations are shifting away from the Multi-Organisational model in 2024 and may need additional guidance from the ISU in completing a PDSP.
- Please reach out to security@ovic.vic.gov.au to discuss your 2024 submission. This includes organisations that have previously participated in the Multi-Organisation process as bespoke PDSP forms need to be generated for you.
- A copy of an updated guide outlining the 2024 Multi-Organisation process will be available on our website later this week.


Primary organisation

Subsidiary organisation

Subsidiary organisation

Subsidiary organisation

Resources

For 2024 PDSP material refer to:

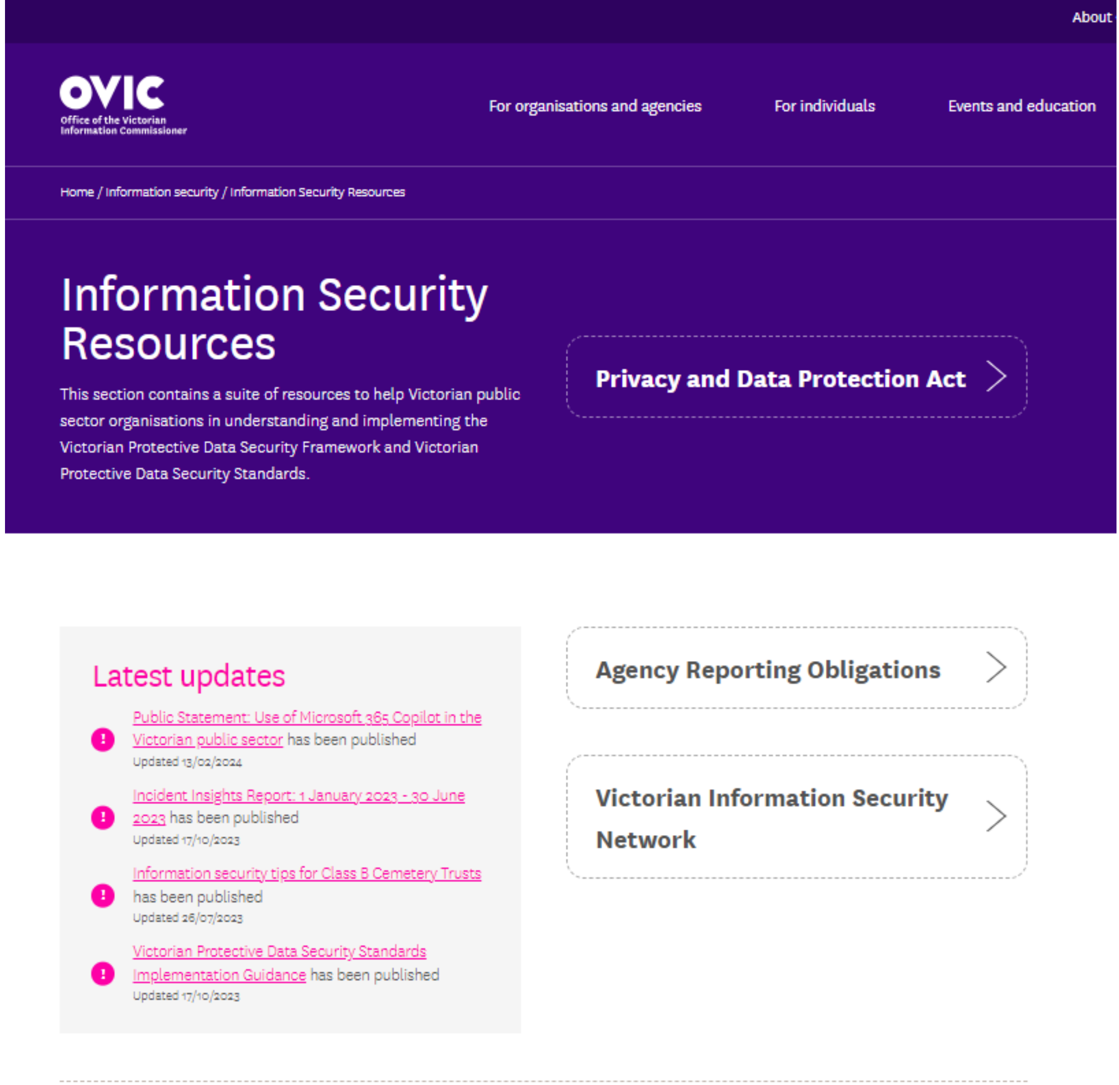
- 2024 PDSP form (V3.4)
- 2024 - How to: A guide to completing the Protective Data Security Plan (PDSP) (V1.3)

For VPDSS elements refer to:

- VPDSS Implementation Guidance (V2.3)
- Implementation Guidance for Industrial Automation and Controls Systems - Extension to VPDSS Implementation Guidance (V1.0)

For guidance on the SRPA process refer to:

- Practitioner Guide – Information Security Risk Management (2.0)



About
OVIC
Office of the Victorian Information Commissioner
For organisations and agencies
For individuals
Events and education

Home / Information security / Information Security Resources

Information Security Resources

This section contains a suite of resources to help Victorian public sector organisations in understanding and implementing the Victorian Protective Data Security Framework and Victorian Protective Data Security Standards.

Privacy and Data Protection Act >

Latest updates

- Public Statement: Use of Microsoft 365 Copilot in the Victorian public sector has been published
  Updated 13/02/2024
- Incident Insights Report: 1 January 2023 - 30 June 2023 has been published
  Updated 17/10/2023
- Information security tips for Class B Cemetery Trusts has been published
  Updated 26/07/2023
- Victorian Protective Data Security Standards Implementation Guidance has been published
  Updated 17/10/2023

Agency Reporting Obligations >

Victorian Information Security Network >

For all other guidance refer to the Information Security Resources page on the OVIC website available at:
https://ovic.vic.gov.au/information-security/information-security-resources/

Questions

Deputy Commissioner - What's next and final thoughts

Office of the Victorian
Information Commissioner

Deputy Commissioner – What's next?

Rachel Dixon
Deputy Commissioner
Privacy and Data Protection

In the first half of 2024 there will be a range of engagement opportunities with the ISU including:

- Incident Insights VISN – April 2024
  - *Registrations for this event to open soon. Keep an eye out on the OVIC events page!*
- PDSP round table events in May/June
- Targeted engagements upon request

To request forms, discuss a significant change, or have any questions answered, reach out to the Information Security Unit via security@ovic.vic.gov.au.

Submit a copy of your PDSP to OVIC between **1 July 2023** and **31 August 2024.**

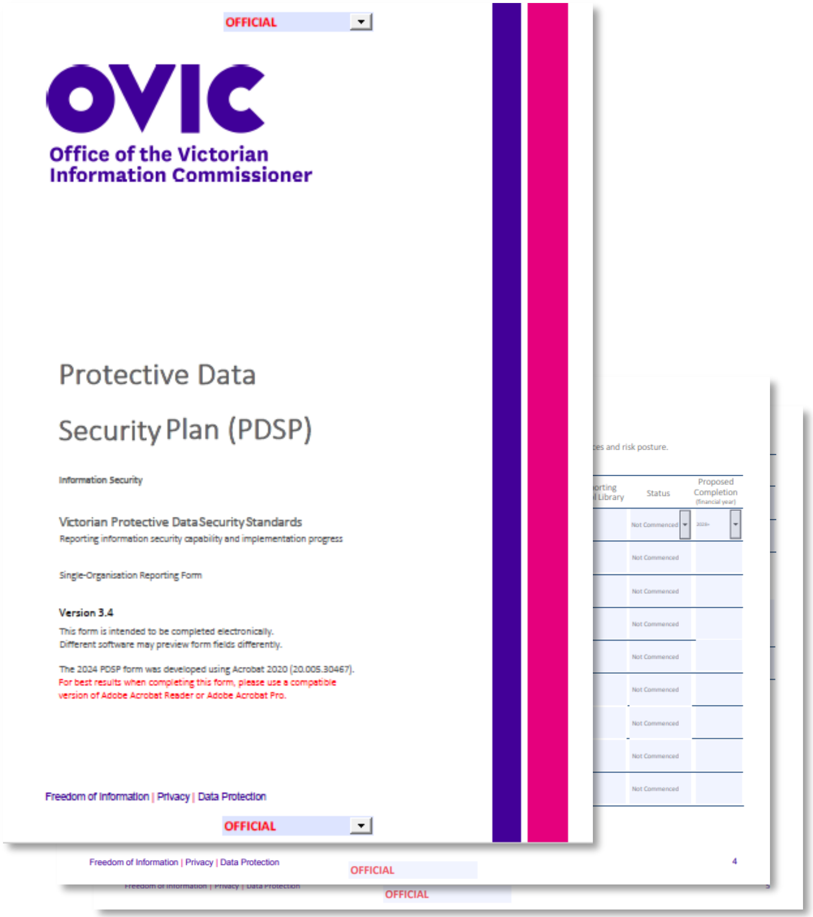
Deputy Commissioner’s – Final thoughts

Rachel Dixon
Deputy Commissioner
Privacy and Data Protection

It’s critical that public sector body Heads are engaged in this process. They are ultimately accountable.

Your responses will help shape important insights and develop future resources.

OVIC appreciate your continued efforts in safeguarding Victoria’s information.



OFFICIAL

Office of the Victorian Information Commissioner

Protective Data Security Plan (PDSP)

Information Security

Victorian Protective Data Security Standards
Reporting information security capability and implementation progress

Single-Organisation Reporting Form

Version 3.4

This form is intended to be completed electronically.
Different software may preview form fields differently.

The 2024 PDSP form was developed using Acrobat 2020 (20.005.30467).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

es and risk posture.

orting l Library	Status	Proposed Completion (financial year)
	Not Commenced	2026-
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	
	Not Commenced	

Freedom of Information | Privacy | Data Protection OFFICIAL 4

Freedom of Information | Privacy | Data Protection OFFICIAL

Thank you

Office of the Victorian
Information Commissioner