Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

2024 - How-to: A guide to the Multi-Organisation Protective Data Security Plan (PDSP) Reporting Model and Process

Freedom of Information | Privacy | Data Protection

Document Details

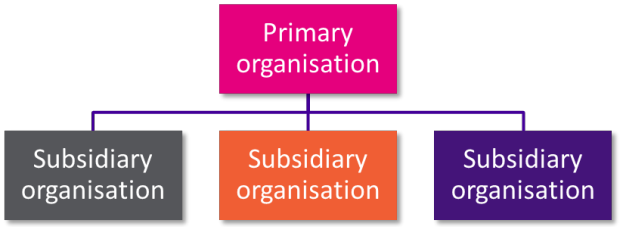
2024 - How-to: A guide to the Multi-Organisation Protective Data Security Plan (PDSP) Reporting Model and Process		
Protective Marking		OFFICIAL
Approved for unlimited public release		Yes – Authorised for release
Release Date		April 2024
Review Date		February 2026
Document Version		1.4
Authority		Office of the Victorian Information Commissioner (**OVIC**)
Author		Information Security Unit – OVIC
Version Control		
Version	**Date**	**Key Changes**
1.0	February 2020	Initial release as an Information sheet
1.1	March 2020	Updated to clarify process flow
1.2	March 2022	Updated to reflect strengthened wording for participants of the Multi-Organisation PDSP reporting process
1.3	February 2024	Updated dates to reflect the 2024 reporting cycle
1.4	April 2024	Updated the 2024 PDSP form version references from V3.4 to V3.5

Contents

Introduction

What is the Multi-Organisation reporting model?

The multi-organisation reporting model is designed to support scenarios where subsidiary organisations have equivalent risk profiles (including appetite and tolerance), risk references, control environments, implementation statuses, completion dates for the Victorian Protective Data Security Standard elements, and maturity levels to those of a primary organisation. In these scenarios the subsidiary effectively operates as a business unit of the primary organisation.

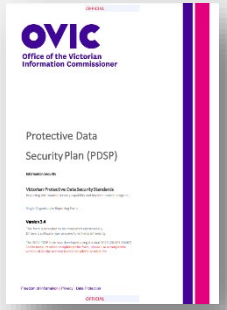


Strengthening the Multi-Organisation reporting model in 2024

Following analysis of the 2018, 2020 and 2022 multi-organisation Protective Data Security Plan (**PDSP**) submissions, OVIC identified a range of issues relating to the identification and management of information security risks of subsidiary organisations versus those of a primary organisation. These issues included different control environments which, in some cases, were not reflected in multi-organisation PDSPs.

To address these issues, in 2022 OVIC implemented a strengthened multi-organisation reporting model. This model requires all organisations (primary and subsidiaries) seeking to use a multi-organisation PDSP to meet certain reporting criteria before proceeding. This model is still in use in 2024.

2024 Primary organisation PDSP (V3.5)



2024 Subsidiary organisation(s) PDSP (V3.4)

Refer to OVIC's **2024 How-to: A guide to completing the PDSP** (V1.3) form for detailed guidance on Part A and B of the PDSP form

Is the Multi-Organisation reporting model appropriate for my organisation?

In the first instance, each subsidiary organisation should liaise with their primary organisation to determine whether the multi-organisation reporting model would be supported. This includes confirming shared reporting criteria with the primary organisation, i.e., that each proposed subsidiary organisation will attest to having equivalent:

a. risk profiles (including appetite and tolerance);
b. control environments;
c. implementation statuses for the elements (including completion dates for VPDSS);
d. risk references; and,
e. maturity levels.

This shared reporting criteria must be met for the subsidiary organisation(s) to be comfortable with their representation on the primary organisation's PDSP form that will be submitted to OVIC.

Should you require further guidance, members of the Information Security Unit are available to discuss. Contact security@ovic.vic.gov.au

When is the Multi-Organisation PDSP due?

The primary organisation must submit a copy of its own PDSP and a copy of each subsidiary's PDSP in a consolidated submission to OVIC between **1 July** and **31 August 2024**. Refer to the Submission and Next Steps section of this guide for submission options.

Steps and Actions Required

STEP	ACTION REQUIRED BY…		
	PRIMARY ORG	SUBSIDIARY ORG	OVIC INFORMATION SECURITY UNIT (ISU)
1	Prior to advising the ISU of an intention to use the multi-organisation reporting model in 2024, primary and subsidiary organisations must collaborate to confirm that the shared reporting criteria is met by all organisations. This includes confirming that each proposed subsidiary organisation can attest to having equivalent: a. risk profiles (including appetite and tolerance); b. control environments; c. implementation statuses for the elements (including completion dates for VPDSS); d. risk references; and, e. maturity levels. This could be undertaken in conjunction with each organisation's Security Risk Profile Assessment (SRPA) process. ⚠ *Where any subsidiary organisation is unable to attest to all shared reporting criteria, the multi-organisation reporting model process is no longer appropriate and a single-organisation PDSP is required. Refer to Agency Reporting Hub for related documents and a current copy of the single-organisation PDSP form.* *In this scenario the subsidiary organisation(s) may still seek assistance from a primary organisation to help complete their single-organisation PDSP.*		

STEP	ACTION REQUIRED BY…		
	PRIMARY ORG	SUBSIDIARY ORG	OVIC INFORMATION SECURITY UNIT (ISU)
2	Advise the ISU of the intention to use the Multi-Organisation reporting model (use the email template provided on page 9 of this guide). This includes providing: • formal confirmation that each proposed subsidiary organisation can attest to the shared reporting criteria; and • details of each subsidiary, including the: - organisation name - public sector body Head's name - public sector body Head's position title - public sector body Head's email address.		
3			1. Create a **tailored primary organisation PDSP** form using the subsidiary organisation(s) details provided. 2. Send a copy of the: a. tailored primary organisation PDSP and b. **the subsidiary organisation PDSP form(s)** to all organisations via email. ⚠ *This correspondence will be one email sent to all organisations listed on the primary PDSP, and outlines who is responsible for completing the required documentation and submission to OVIC.*

STEP	ACTION REQUIRED BY…		
	PRIMARY ORG	SUBSIDIARY ORG	OVIC INFORMATION SECURITY UNIT (ISU)
4	1. Collaborate with each subsidiary organisation(s) to reflect each subsidiary organisation's risks and controls on the primary organisation PDSP form. a. This could be undertaken in conjunction with the Security Risk Profile Assessment (SRPA) process. 2. Develop primary organisation PDSP form. 3. Confirm each subsidiary organisations' representation on the primary organisation PDSP form.	Collaborate with primary organisation to ensure its risks and controls are reflected on the primary organisation PDSP form.	
5	Provide input/assistance to each subsidiary to complete their subsidiary PDSP form.	Complete the subsidiary organisation PDSP form.	
6	Finalise and sign the tailored primary organisation PDSP form.	1. Finalise and sign the Subsidiary organisation(s) PDSP form. 2. Send to the primary organisation.	
7	1. Collate all signed PDSP forms (primary and subsidiary organisation PDSP forms). 2. Submit to OVIC between 1 July - 31 August 2024 ensuring any subsidiary organisations are copied in on this correspondence.		
8			Confirm receipt of the PDSPs with the primary organisation and subsidiary organisations.

Sample Email Template for **Primary** Organisation to send to ISU (step 2 of Multi-Organisation reporting process)

TO:	security@ovic.vic.gov.au
CC:	*[include any relevant contacts]*
SUBJECT:	Intention to use Multi-Organisation PDSP reporting model in 2024
CONTENT:	**Attention**: Information Security Unit I am confirming that *[insert primary organisation name]* and *[insert subsidiary organisation name(s)]* intend to use the Multi-Organisation reporting model in 2024. 1. I can confirm that the subsidiaries listed below (in point 2) can attest to having equivalent: a. risk profiles (including appetite and tolerance); b. control environments; c. implementation statuses for the elements (including completion dates for VPDSS); d. risk references; and e. maturity levels. 2. Details of each subsidiary organisation(s): • Subsidiary organisation name: *[Insert subsidiary organisation name]* • Public sector body Head's name: *[insert name of public sector body head of the subsidiary organisation]* • Public sector body Head's Position title: *[insert title of public sector body head of the subsidiary organisation]* • Public sector body Head's email address: *[insert email address of public sector body head of the subsidiary organisation]* *[If you need to add additional subsidiaries, please copy and paste item 2 and complete the corresponding details]* *[Ensure you include your email signature with your contact details and role title should the ISU have any follow up questions]*

Submission and Next Steps

Options for submission

When all mandatory fields on the PDSPs have been completed and the public sector body Heads have reviewed the form, signed and dated the Attestation the primary organisation submits a copy of the collated PDSP to OVIC via one of the options below.

Note: Remember to retain a copy of the completed PDSP for organisational records.

For PDSPs marked as OFFICIAL and OFFICIAL: Sensitive **Please note:** A prior appointment must be made with a member of OVIC's Information Security Unit for option 3.	**Option 1**	Soft copy / electronic	Send a copy of the completed, signed and dated PDSPs to security@ovic.vic.gov.au (either from the public sector body Head's email address, or the Information Security Lead's email address)
	Option 2	Hard copy	Post a copy of the PDSP in a single opaque envelope with no protective marking labelled on the outside to: PO Box 24274 Melbourne VIC 3001
	Option 3	Hard copy	Hand deliver a copy of the PDSP to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne VIC 3001
For PDSPs marked as PROTECTED **Please note:** A prior appointment must be made with a member of OVIC's Information Security Unit for options 4 and 5.	**Option 4**	Hard copy	Deliver a copy of the PDSP by safe-hand (e.g. delivered in person by an authorised messenger) to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne
	Option 5	Hard copy	Deliver a copy of the PDSP by SCEC-endorsed courier to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne

Next steps

After submitting the PDSP to OVIC the organisation will receive an email confirming receipt by OVIC's Information Security Unit within 1-15 business days.

Between now and the next OVIC reporting period ensure the organisation continues to:

- monitor the organisation's information security risks;
- alert OVIC to any significant changes to the organisation's information security risks and/or operating environment;
- notify OVIC of any changes to the organisation's Information Security Lead and/or public sector body Head; and
- report information security incidents through the Incident Notification Scheme.