OVIC

**Office of the Victorian
Information Commissioner**

INFORMATION FOR
AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

How-to: A guide to the 2022 Multi-Organisation

Protective Data Security Plan (PDSP) Reporting Model and Process

Document Details

| How-to: A guide to the 2022 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	March 2022
Review Date	January 2024
Document Version	1.2
Authority	Office of the Victorian Information Commissioner (**OVIC**)
Author	Information Security Unit - OVIC

Contents

Freedom of Information | Privacy | Data Protection

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.
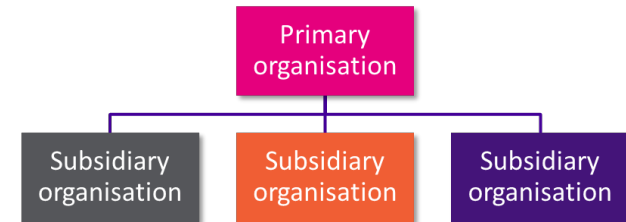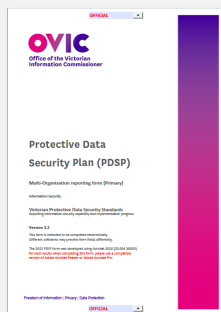

Strengthening the Multi-Organisation reporting model in 2022

Following analysis of the 2018 and 2020 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, OVIC has implemented a strengthened multi-organisation reporting model in 2022. This model requires all organisations (primary and subsidiaries) seeking to use a multi-organisation PDSP to meet certain reporting criteria before proceeding.

Primary organisation PDSP	Subsidiary organisation(s) PDSP	Refer to OVIC's How-to: A guide to completing the 2022 PDSP form for detailed guidance on Part A and B of the PDSP form

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

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?

A consolidated submission of the primary organisation and subsidiary organisation(s) PDSPs is due to OVIC by **31 August 2022**. Refer to the Submission and Next Steps section of this guide for submission options.

Freedom of Information | Privacy | Data Protection

INTRODUCTION

Steps and Actions Required

STEP	ACTION REQUIRED		
	PRIMARY ORG	**SUBSIDIARY ORG**	**OVIC INFORMATION SECURITY UNIT (ISU)**

1	The shared reporting criteria must be met by all organisations (primary and subsidiary) prior to advising the ISU of their intention to use the multi-organisation reporting model in 2022.
	
	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.
	
	⚠️ *Where any subsidiary organisation is uncomfortable or 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 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.		

Freedom of Information | Privacy | Data Protection

STEPS AND ACTIONS REQUIRED

STEP	ACTION REQUIRED		
	PRIMARY ORG	**SUBSIDIARY ORG**	**OVIC INFORMATION SECURITY UNIT (ISU)**
2	Advise the ISU of the intention to use the Multi-Organisation reporting model. This includes providing: • formal confirmation that each proposed subsidiary organisation can attest to the shared reporting criteria • 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. *A sample email template for this step is included on page 9 of this How-to Guide.*		
3			a. Create a **tailored primary organisation PDSP** form using the subsidiary organisation(s) details provided. b. Send a copy of the tailored primary organisation PDSP and **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.*

Freedom of Information | Privacy | Data Protection

STEPS AND ACTIONS REQUIRED

STEP	ACTION REQUIRED		
	PRIMARY ORG	**SUBSIDIARY ORG**	**OVIC INFORMATION SECURITY UNIT (ISU)**
4	a. Collaborate with each subsidiary organisation(s) to reflect each subsidiary organisation's risks and controls on the primary organisation PDSP form. • This could be undertaken in conjunction with the Security Risk Profile Assessment (**SRPA**) process. b. Develop primary organisation PDSP form. c. Confirm each subsidiary organisations' representation on the primary organisation PDSP form.	a. Collaborate with primary organisation to ensure its risks and controls are reflected on the primary organisation PDSP form. • This could be undertaken in conjunction with the Security Risk Profile Assessment (**SRPA**) process.	
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.	Subsidiary organisation(s) provide a signed copy of the subsidiary organisation PDSP form to the primary organisation.	
7	Collate all signed PDSP forms (primary and subsidiary organisation PDSP forms) and submit to OVIC by 31 August 2022 including (in CC) any subsidiary organisations.		
8			Confirm receipt of the PDSPs with the primary organisation and subsidiary organisations.
Each organisation satisfies their reporting obligations for 2022.			

STEPS AND ACTIONS REQUIRED

Freedom of Information | Privacy | Data Protection

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 2022
CONTENT:	**Attention**: Information Security Unit

CONTENT: continued:

I am confirming that *[insert primary organisation name]* and *[insert subsidiary organisation name(s)]* intend to use the Multi-Organisation reporting model in 2022.

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.

b. 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]

Freedom of Information | Privacy | Data Protection

Submission and Next Steps

Options for submission

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

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	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 the PDSPs 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 the PDSPs 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 the PDSPs 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 the PDSPs by SCEC-endorsed courier to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne
For PDSPs marked as **SECRET**	**Option 6**		If the PDSPs are assessed as containing security classified information as **SECRET**, please speak to a member of OVIC's Information Security Unit to discuss further.

Freedom of Information | Privacy | Data Protection

Next steps

After submitting the collated PDSPs to OVIC, each 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, all organisations represented on the primary organisation PDSP form must continue to:

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

Freedom of Information | Privacy | Data Protection