

Significant Change under Part 4 of the Privacy and Data Protection Act (2014)

Victorian Protective Data Security Framework and Standards

Overview

This information sheet explains:

- what may constitute a significant change to an organisations operating environment or information security risks;
- what to do when an organisation identified that there may be significant change; and
- when OVIC expects to be notified of significant change and receive a revised Protective Data Security Plan (**PDSP**).

Under the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**), organisations must undertake a Security Risk Profile Assessment (**SRPA**) and develop a PDSP. A copy of this completed PDSP must be given to the Information Commissioner:

- within 2 years of the issue of the Victorian Protective Data Security Standards (**VPDSS**); or
- **upon significant change** to the operating environment or security risks to the organisation.

What constitutes a significant change?

It is difficult to define significant change. It depends on the type of change, information security risks relating to the change, and the organisation's operating context. Some examples of significant change could include situations where **information security risks** have changed due to one or more following:

- Machinery of Government (**MoG**) changes to the organisation's structure or information assets / systems;
- high staff turnover or changes to staffing (e.g., major organisational restructures);
- changes resulting from new or amended legislation;
- changes to work functions or business operations;
- changes in the operating environment of the organisation (like a large scale move to remote working);
- changes to an information system, or the introduction of a new system (including where a third-party provider manages this system on behalf of the organisation); or
- changes to service provider arrangements, where the provider accesses, uses or manages information or information systems on behalf of the organisation (e.g., CenITex as a shared service provider to manage the organisation's ICT network).

When significant change occurs, organisations must assess the impact of the change and have an informed discussion with OVIC about their information security obligations.

What should my organisation do when it identifies a potential significant change?

When an organisation identifies a potential significant change, it should:

1. Contact the Information Security Unit (ISU) within 30 days to discuss next steps;
2. Consult with any impacted parties, complete the **Notification of Significant Change** form¹ (**Appendix A**) and send the form to security@ovic.vic.gov.au;
3. Undertake a SRPA to capture new or changed information security risks, reflecting these changes in the organisation's risk register;
4. Revise the organisation's PDSP to capture new or changed information security risks, update the activities to address the VPDS and update the implementation status for the activities; and
5. Submit a copy of the revised PDSP to the Information Commissioner.

Who notifies the Information Commissioner of a significant change?

The public sector body Head should submit the **Notification of Significant Change** form to the Information Commissioner.

What are my organisation's continuing reporting obligations?


Deliverable	Timeframe
Undertake (and/or) update a SRPA for the organisation.	Annual <i>(at least)</i>
Provide OVIC with an Attestation by the public sector body Head.	Annual
Submit a PDSP (including an Attestation) by the public sector body Head.	Biennial <i>(every 2 years)</i>
Submit an updated PDSP to OVIC, if there is significant change to the: <ul style="list-style-type: none">• operating environment of the VPS organisation; or• security risks relevant to the VPS organisation.	In consultation with OVIC
Notify OVIC of any information security incidents that compromise the confidentiality, integrity, or availability of public sector information, with a 'limited' business impact or higher, on government operations, organisations or individuals ² .	As required

Please note: Organisations submitting an 'out of cycle' PDSP, must continue to adhere to the regular reporting cycle as outlined in Section 8 of the VPDSF.

¹ Download the [Significant Change Notification Form](#).

² Find out more about incident notification on [OVIC's website](#).

Appendix A – Notification of Significant Change form



Office of the Victorian
Information Commissioner

FORM FOR
AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

Form: Notification to the Information Commissioner of Significant Change

Victorian Protective Data Security Framework and Standards

Notification to the Information Commissioner of Significant Change

Under section 8D(2)(b) of the Privacy and Data Protection Act 2014 (the PDP Act) and Standard 9 of the Victorian Protective Data Security Standards (the Standards).

I _____ am authorised to notify the Information Commissioner that (my "organisation") _____ has identified significant change in its operating environment or significant change in its security risks relevant to the agency or body, as set out below:

Description of change	
Impacted organisation and parties	

My organisation is managing interim risks associated with this significant change and will:

1. undertake a Security Risk Profile Assessment (SRPA);
2. review its Protective Data Security Plan (PDSP); and
3. give a copy of the PDSP to the Information Commissioner under sections 89(4)(a) and 89(5) of the PDP Act by _____ (insert agreed date).

Signature:
Print name:
Position:
Date:

Freedom of Information | Privacy | Data Protection

Download a copy of the [Significant Change Notification Form](#).

Further Information

Contact Us

t: 1300 00 6842
e: security@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer

This fact sheet does not constitute legal advice and should not be used as a substitute for applying the provisions of the Freedom of Information Act 1982 Privacy and Data Protection Act 2014, or any other legal requirement, to individual cases.