Significant change and protective data security obligations

Overview

Under the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**), agencies and bodies are required to undertake a Security Risk Profile Assessment (**SRPA**) and develop a Protective Data Security Plan (**PDSP**).

Agencies and bodies must undertake an SRPA and submit a copy of their PDSP to the Office of the Victorian Information Commissioner (**OVIC**):

- 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 agency or body.

This information sheet addresses significant change considerations, and OVIC's expectations in receiving a copy of a revised PDSP.

What is significant change?

It is difficult to define significant change as it depends on the context of each individual agency and their individual situation.

Some examples of situations that may constitute significant change include:

- Machinery of Government changes;
- significant staff turnover or changes to staffing (e.g. restructures);
- changes imposed by the introduction or amendment of legislation;
- changes to work functions or business operations;
- changes in the operating environment of the organisation (such as a large scale move to remote working); or
- introduction or removal of information systems or third parties that have a considerable impact on the agency's information assets (for example, the use of CenITex as a shared service provider to manage the agency's network).

For the purposes of information security, OVIC is focused on the security risks to the agency's information assets. Agencies should consider the impacts of the change (e.g. the extent and duration) and have an informed discussion with OVIC about their protective data security obligations.

What does my agency need to do if we have experienced significant change?

Once an agency has experienced significant change, they are required to notify OVIC *within 30 days of the change being identified*.

Following consultation, the agency may be required to:

1. Undertake an updated SRPA, capturing any new or changed information security risks in the agency's risk register;

2. Revise the agency's PDSP, capturing any new or changed information security risks and updated programs of work; and

3. Provide a copy of the updated PDSP and attestation to OVIC's Information Security Unit.

Ongoing reporting cycles

When significant change occurs, it is often beyond our control. This may have other implications including ongoing PDSP/attestation reporting cycles to OVIC. If you experience significant change, OVIC's Information Security Unit can advise on reporting timeframes within the standard 2 year reporting cycle.

Further Information

Agencies can find additional information and resources on the VPDSF Resources page on the OVIC website. Information security practitioners may also request access to the Victorian Information Security Network (**VISN**) for additional practitioner guides and to engage with other members across the Victorian Public Sector and industry partners. To become a member of the VISN, please contact the Information Security Unit.

Contact Us

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

Disclaimer