Victorian Protective Data Security obligations during COVID-19

Victorian Protective Data Security Framework and Standards

Overview

OVIC recognises that COVID-19 has caused considerable impacts on the general public and Victorian public sector (**VPS**) organisations. We are all facing disruptions to our day to day lives and trying to manage new ways to work, often remotely.

While we adapt to new ways of working, VPS organisations must continue to manage information security risks to their information assets. This information sheet addresses three frequently asked questions on information security during this time.

Frequently asked questions

1. **Can I get an extension on undertaking a Security Risk Profile Assessment (SRPA) and submitting a Protective Data Security Plan (PDSP) by August 2020?**

   OVIC cannot provide extensions or exemptions as there are no legislative provisions to do so under the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

   The PDP Act requires VPS organisations to:

   - adhere to the Victorian Protective Data Security Standards (**VPDSS**);
   - undertake a SRPA; and
   - develop, implement and maintain a PDSP.

   Organisations managing a remote workforce often find themselves having to find new ways of working whilst maintaining the security of their information assets. Now more than ever, organisations must monitor and manage their information security risks.

   To effectively manage the current threat environment, organisations should undertake the SRPA process. The SRPA process should be conducted at least annually.

   Any new or amended risks identified during the SRPA process must be reflected in the organisation's 2020 PDSP. Any new activities required to address these new or amended information security risks should also be captured on the PDSP.

   We understand that in this current environment, certain programs of work supporting implementation of the VPDSS may be put on hold or will be noted as incomplete for this reporting period. Keep in mind the PDSP is simply a reflection of your organisation's current information security program and future planning, so if you do experience challenges due to COVID-19, please list these on the PDSP.

April 2020 – Version 1.0

SRPA	Step by step instructions on how to undertake a SRPA are outlined in the Practitioner Guide: Information Security Risk Management available on OVIC’s website.
PDSP	To find a current copy of the PDSP template please refer to the PDSP submission page on OVIC’s website.

2. **Do I still need to notify OVIC of information security incidents within 30 days of identifying the incident?**

   Yes. VPS organisations are still required to notify OVIC of information security incidents within 30 days of being identified.

   With most organisations moving to remote working arrangements as a result of COVID-19, new information security risks must be managed. Some of these risks may result in an incident. Incidents that may arise in the current environment could include leaving sensitive hard copy documents on a desk at home that may result in members of the household accessing them, someone breaking into a remote work environment and stealing sensitive documentation, or a sensitive conversation being overheard in a household.

   For more information on the Information Security Incident Notification Scheme, refer to the Incident Notification page on OVIC’s website.

3. **Do I have to meet the October 2020 deadline for implementing the new protective marking scheme?**

   The October 2020 deadline for the implementation of the new protective marking’s scheme is not a compliance directive by OVIC. The October 2020 date is outlined under the Commonwealth Protective Security Policy Framework (**PSPF**) and Information Security Manual (**ISM**). OVIC is not aware of any extensions or exemptions being granted.

   VPS organisations should try to meet this target if it is within their resources to do so. However, organisations that do not meet this timeline must manage the associated risks and implement any mitigation strategies when sharing information with entities operating under the new scheme post October 2020.

   These include potential limitations in exchanging emails with other government organisations, or issues with personnel actively using material that is either inappropriately marked or potentially unmarked. For resources on the new protective marking scheme, refer to the VPDSF Resources page on OVIC’s website.

Further information

Join the Victorian Information Security Network (**VISN**) for more resources and to engage with other information security professionals. Contact the Information Security Unit to join.

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.