Office of the Victorian Information Commissioner

Victorian Information Security Network (VISN) Forum

10 February 2022

Questions	Answers/Responses
Do organisations that did a full report (Protective Data Security Plan (PDSP)) late last year as a result of a significant change need to do another full report this year?	Organisations that submitted an 'out of cycle' PDSP as a result of significant change are still required to submit an updated PDSP by August 31, 2022. Hopefully this exercise won't be overly onerous and will be a matter of sense checking how you were positioned when you last submitted and if any tweaks need to be made to this submission. Keep in mind, the PDSP form has changed - refer to https://ovic.vic.gov.au/wp-content/uploads/2022/02/2022-Single-Organisation-Protective-Data-Security-Plan-PDSP-form-V3.1.pdf for the most recent release of this form.
What is expected by OVIC in reference to the Security Risk Profile Assessment (SRPA)? Is there a document output or assurance that risks are identified, captured and managed?	To find out how to undertake the Security Risk Profile Assessment (SRPA) process, refer to our Practitioner Guide on Information Security Risk Management. https://ovic.vic.gov.au/data-protection/practitioner-guide-information-security-risk-management/ Outcomes of the SRPA process should be documented in the organisations risk register and particular fields on the PDSP form (e.g. entity risk reference(s), supporting control library, status and proposed completion).
The SRPA is a process not an output document that's submitted to OVIC?	Correct, the SRPA is a process that all in-scope organisations must undertake, as required under Part 4 of the Privacy and Data Protection Act 2014.

	It is not a document that needs to be submitted to OVIC. The only documentation that needs to be submitted to OVIC by 31 August 2022, is an updated PDSP. As above, outcomes of the SRPA process should be documented in the organisations risk register and particular fields on the PDSP form (e.g. entity risk reference(s), supporting control library, status and proposed completion). For more info on how to record these outcomes in the PDSP form, check out the new 'How To Guide' - https://ovic.vic.gov.au/wp-content/uploads/2022/01/How-to-A-guide-to-completing-the-2022-Protective-Data-Security-Plan-PDSP-form-V1.0.pdf
My organisation has a major project lined up for August which will impact us significantly. Will we have to re-submit our report after or can the Aug deadline be extended?	Please shoot an email to security@ovic.vic.gov.au so we can set up a time to discuss your requirements.
Can use existing risk management framework right?	Yes – We suggest you use your existing risk management framework.
Do we need to request a specialised PDSP template for those organisations which are multi-organisations from OVIC?	Yes, our team has to create a bespoke Multi-Org form for the entities that are looking to consolidate their reporting. Please reach out to security@ovic.vic.gov.au to arrange a time to discuss your approach with us.
Is there a new Cemetery Trust Template available?	Please check out the new Class B cemetery trust page where you can download the form. Across the next couple of weeks our team will also send out hard and soft copies of this material to Class B cemetery trust stakeholders. This material is not to be used by Class A cemetery trusts or other VPS organisations. https://ovic.vic.gov.au/agency-reporting-obligations-hub/class-b-cemetery-trust-stakeholders/

Any changes to multi-org forms and submit process?	For all multi-organisation requests, please email security@ovic.vic.gov.au as there will be reporting nuances that need to be discussed with our team.
Can you provide guidance or library on a list of controls / risk mitigations and levels of risk they address (e.g. a more extreme risk, type of risk and what controls universe is relevant)?	The VPDSS elements are essentially the basis for your control library to mitigate your risks. OVIC cannot rate the organisational risks they address as it will depend on your business and supporting environment. If you require assistance in assessing risk, reach out to VMIA or 'like' organisations.
Is it possible to get the form (PDSP) in a word or excel format pls?	The 2022 PDSP form for VPS organisation is only available in PDF. If you have adobe acrobat pro there may be export options to a spreadsheet which may assist.
When will element maturity automatically generate the Standard status?	Product enhancements, including options for systems (which would help automate some functions and analysis) are always being considered. Unfortunately, this will not be available for this reporting period. At the moment we are limited to filling PDFs.
Is it possible to have "Ongoing" as a status? "Completed" can sometimes be too comfortable and further work in the space may be challenged. This is especially for areas of Education and awareness that needs to be done on a continuous basis.	We have accommodated for business as usual (BAU) activities in the new PDSP form. Select 'completed/BAU' under proposed completion field to indicate this status.
Essential 8 - Cyber threat controls	Essential 8 controls are referenced (albeit not always overtly listed) and woven through the Elements of Standard 11. If you need clarification on any of these, please email security@ovic.vic.gov.au
For the questions around 'How was this form validated', can we select combinations of a couple of methods (i.e.	If you have undertaken more than one method to validate the responses on your PDSP then feel free to tick more than one box.

some internal, self-assessed, and private audit validations). Meaning tick more than one box?	
IACS - if we have these in an education lab environment, not in production, should that be a Yes or a No?	Great question Jason – please email security@ovic.vic.gov.au to see if the organisation needs to consider the additional IACS questions.
Can we do digital signoff for the signature or does it need to be a physical signature from the body head?	Signature / sign off options are outlined in the How To Guide. This includes options for soft copy and hard copy sign off.
Do you have the link for the PDSP Executive Presentation?	Check out this briefing pack designed to brief executives and leadership: https://ovic.vic.gov.au/data-protection/information-security-general-executive-briefing-pack You may also want to show your executive the video from our Commissioner which speaks to the public sector body Head's obligations in 2022 - https://vimeo.com/670515157
What determines the protective markings of the submission?	An assessment of the security value of the responses recorded in the organisation's PDSP form will inform the relevant protective marking for this year's submission.
Almost our entire team has changed since this would have last been done. Our team is also very small. It's difficult to gauge how much time/effort this will require.	If possible, we sincerely recommend you start early especially if the team is unfamiliar with the process. If you have questions as you go, reach out to security@ovic.vic.gov.au
I'd been using the DHHS Info Security Sharepoint site as a source of information. Are the updates to the document available there, or should i switch to the OVIC website as the primary source of info?	Without having visibility of what is captured on the DHHS Info Security Sharepoint site, it's hard for us to comment on this. Users should refer to their internal security policies and procedures in the first instance and seek direction from their internal security teams (if they have them).

	All VPDSS / VPDSF resources are available on the OVIC website for anyone to access and use and will include the most up to date resources to help you out. Check out https://ovic.vic.gov.au/data-protection/information-security-resources/ For our VPS stakeholders seeking updated resources relating to 2022 reporting requirements please check out our refreshed page- https://ovic.vic.gov.au/agency-reporting-obligations-hub/vps-stakeholders/. A copy of the 2022 VPS PDSP form, 2022 VPS How-to Guide, and video from our commissioner can be found there!
What are your feelings around the use of Microsoft 365 Compliance Manager VPDSS template?	As a regulator we can't comment on specific tools as such. Feel free to reach out to security@ovic.vic.gov.au if you are looking to have a fuller discussion around assessment tools and approaches.
How to guide can you provide link please?	To access and download the 2022 How-to Guide: A guide to completing the 2022 Protective Data Security Plan check out https://ovic.vic.gov.au/wp-content/uploads/2022/01/How-to-A-guide-to-completing-the-2022-Protective-Data-Security-Plan-PDSP-form-V1.0.docx
You mentioned s89 of the PDP Act at the beginning i.e. that "A security risk profile assessment of an agency or body must include an assessment of any contracted service provider of the agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body." Where "public sector data" is defined in the PDP Act as "any information (including personal information) obtained,	The definition of public sector data under the PDP Act is very very broad. It is not limited to personal information, financial information, health information, etc. but rather (as you noted) **ANY** information (including personal information) obtained, received or held by an agency or body to which Part 4 applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body. Public sector data is defined by context (i.e. consider the applicability of the entity under Part 4 of the PDP Act, irrespective of the type of information they obtain, receive or hold).

received or held by an agency or body to which Part 4 applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body;" Does this definition also include data in the public domain or is it more narrowly scoped to Personally identifiable information, financial information, health information, etc?	

Further helpful resources	
2022 PDSP form (v 3.1)	Download the 2022 PDSP v3.1 here: https://ovic.vic.gov.au/wp-content/uploads/2022/02/2022-Single-Organisation-Protective-Data-Security-Plan-PDSP-form-V3.1.pdf
VPS 2022 How-to Guide	Check out the 2022 How-to Guide: A guide to completing the 2022 Protective Data Security Plan here: https://ovic.vic.gov.au/wp-content/uploads/2022/01/How-to-A-guide-to-completing-the-2022-Protective-Data-Security-Plan-PDSP-form-V1.0.docx
2022 Video from OVIC Commissioner	To watch the 2022 video from the Victorian Information Commissioner please go to https://ovic.vic.gov.au/agency-reporting-obligations-hub/vps-stakeholders/
VPS Hub	Head to https://ovic.vic.gov.au/agency-reporting-obligations-hub/vps-stakeholders/
Executive briefing pack	Briefing pack designed to brief executives and leadership: https://ovic.vic.gov.au/data-protection/information-security-general-executive-briefing-pack

Security Risk Profile Assessment (SRPA) guidance	To find out how to complete the Security Risk Profile Assessment (SRPA) process, refer to our Practitioner Guide on Information Security Risk Management: https://ovic.vic.gov.au/data-protection/practitioner-guide-information-security-risk-management/
VMIA material	VMIA's updated risk guidance materials for a start if anyone is new to VMIA Practical guidance for managing risk | Victorian Managed Insurance Authority (vmia.vic.gov.au)
VPDSS Glossary (v2.1)	Victorian Protective Data Security Standards Glossary v2.1 https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-standards-glossary-v2-1/
VPDSS Implementation Guidance (v2.1)	Check out the VPDSS Implementation Guidance V2.1 here: https://ovic.vic.gov.au/wp-content/uploads/2021/02/20210216-VPDSS-V2.0-Implementation-Guidance-V2.1.pdf
Top Questions for the Audit Risk Committee	Check out the Fact Sheet Top Questions for the Audit Risk Committee: https://ovic.vic.gov.au/data-protection/top-questions-for-the-audit-and-risk-committee