Victorian Protective Data Security Standards (VPDSS) V2.0

Consultation Questions and Answers

Thank you to all who provided OVIC with valuable feedback during the consultation of our draft updated standards. Your input has helped shaped the new version 2.0. We have correlated some frequently asked questions and answers received during the VPDSS consultation period for our stakeholders to gain an insight into our development and delivery of VPDSS V2.0.

Question/Comment	OVIC response
Changing the language used throughout to active voice and removing 'must'	Most submissions supported this change. Stakeholders felt the updated wording was easier to understand across the business and 'must' was not required given the VPDSS is already mandated under the Privacy and Data Protection Act.
Introducing incident notification under the new Standard 9	Most submissions supported this change. Stakeholders felt this wasn't too onerous as they already have reporting obligations for incidents currently or understand this is the natural role of regulators so this would just be another party to add in an organisation's incident response plan. Most of the questions around incident reporting were around the detail i.e. what, when, who and how. OVIC is in the process of developing some supporting guidance related to how this will operate in practice.
Including the sources from which the standards have been derived	This was a welcomed addition to the detailed VPDSS implementation guide, reducing the number of documents stakeholders had to navigate to when seeking implementation guidance.

Question/Comment	OVIC response
Add 'based on the organisation's risk appetite/tolerance' to each of the elements.	Risk management is an underlying principle of the VPDSS as detailed in the VPDSF. Applying the VPDSS requires an understanding of the organisation's risk posture as stated in many of the Standards themselves. Rather than adding 'based on risk' to every element, the section 'A word on the elements' has been updated to explicitly call out up front that the overall application of all the elements needs to take into consideration the following three criteria: internal and external context; the security value of the information; and associated risks.
Can you please add reference to additional resources?	OVIC has referenced the primary source documents used for each element to give further information regarding implementation. OVIC is happy to explore the development of a supplementary resource list for practitioners. Organisations are encouraged to create their own internal control library, which can reference additional sources beyond those offered under the VPDSS.
How would implementation of element '*X*' look like? Would '*X*' be sufficient?	Implementation of elements will vary from organisation to organisation. One organisation may have a big documentation set with separate documents (policies, procedures) for each topic area, or specific tools to capture and manage their risks/information assets, another organisation may have a single document, a checklist, a spreadsheet.

Question/Comment	OVIC response
Please use freely available primary sources.	The identified primary sources are available free of charge for the VPS either through the source's direct website or for Australian Standards, through the Victorian Government Library Service for eligible VPS organisations.
Please explain the term 'internal control library'.	A list of controls used by the organisation to secure information. This may be a single control set from a single source e.g. AS/ISO 27002 or be derived from a variety of sources that the organisation uses. Note - some organisations may use the VPDSS elements as their internal control library.
What is the difference between a 'security risk profile assessment' and 'security risk assessments'?	These are essentially equivalent and describe the same process of identifying, analysing, evaluating and treating risks. OVIC has modified the information security risk management standard and supporting elements to clarify this terminology.
What is a risk register?	Refer to the VPDSF Glossary and VMIA Resources. A record of the results of information security risk assessments and treatment plans. This may take the form of a document, spreadsheet, software application.
Define the word 'regular'	Updated to provide a nominal timeframe e.g. at least annually.
Move the Information Security Value Standard up to Standard 2 for logical sequencing in line with the 5-step action plan of identify assets and value them before conducting a risk assessment.	In the updated VPDSS, OVIC has moved the sequencing of this Standard for logical flow. It is now Standard 2.

Question/Comment	OVIC response
Should the Protective Data Security Plan (PDSP) be called an information security plan?	Where changes to the term 'information security' can be made they have been, however the PDSP is specifically described in legislation using these terms and, as such, has not been changed.
What does 'regularly reviews its threat environment' mean?	This relates to keeping up to date with any: • changes to the operating environment which may present opportunities for the organisation to be compromised; • new vulnerabilities that may be exploited; and • threat actors that the organisation should be aware of. The organisation should monitor the risks to their information assets, to see if any changes are required to manage these. In the updated VPDSS, this element has been removed, as it is implicitly covered as part of the organisation monitoring and reviewing its information security risks.
What does 'track access to key/important information' mean?	This relates to an organisation making sure they know the movements of their 'crown jewels' including where important key/ information is stored, who has access to it, etc. In the updated VPDSS, this element has been removed at this time as part of this is covered through other elements such as information asset register and information sharing agreements.

Question/Comment	OVIC response
What are physical and logical access controls?	In the updated VPDSS, examples have been added to these elements. They include: - physical access controls (e.g., key management, swipe card access, visitor passes) - logical access controls (e.g., network account, password, two-factor authentication)
What do you mean by 'all persons'?	Refer to the VPDSF Glossary. 'Employees, volunteers, contractors / sub-contractors and consultants (whether directly or indirectly engaged)' This is purposefully drawn out because who has access to the organisation's information goes beyond staff.
What is meant by information security incident management covering all security areas?	When implementing information security incident management consider beyond just incidents relating to ICT as incidents can extend to compromises of hard copy information or inappropriate verbal disclosure. It also acts as a prompt for organisations to consider controls to mitigate the reoccurrence of the incident beyond ICT controls, considering other security areas of personnel security, physical security and ICT security.
Can you add more / change the incident management phases?	The incident management phases follow the stages extracted from the Australian Standard primary source *AS ISO/IEC 27035.1:2017 Information security incident management Part 1: Principles of incident management* Organisations can add/change these phases as required to suit their environment.

Question/Comment	OVIC response
Define 'third party'	Refer to the VPDSF Glossary. This includes any external party outside of the organisation and can be another government organisation or a contracted service provider.
Under the third-party arrangements Standard, why were these terms 'collect, hold, manage, use, disclose or transfer' listed and not others?	These terms are straight out of the definitions in the PDP Act under the term 'handling' on page 5.
Under the third-party arrangements Standard, reconsider the term 'ensures' a third party securely handles information.	This term is consistent with Part 4 of PDP Act which states 'ensure' As per Part 4 of PDPA the onus rests on the agency head.
Is the term 'official information' only related to information assessed at business impact level (BIL) 2?	With the recent protective marking reforms and the introduction of the 'OFFICIAL' protective marking, this has generated some confusion around whether the VPDSS relates to all forms of official information or just information assessed at the OFFICIAL protective marking level. The VPDSS applies to ALL public sector information handled by organisations to which Part 4 of the PDP Act applies regardless of protective marking. In the updated VPDSS, the term 'official information' has been replaced with 'public sector information' to address this.

Question/Comment	OVIC response
What do you mean by the term ‘information release’?	Refer to the VPDSF Glossary. Information release refers to where the organisation has authorised the uncontrolled dissemination of their information, or publication on various public platforms e.g. website, social media, news, DataVic. Information release (where you release control of what is done with the information) differs from information sharing which involves some form of control. Information sharing is where the owning organisation identifies the handling requirements that the receiving organisation must follow in order to provide the information owner with assurance that the information is handled as they would expect. Prior to releasing or sharing information, organisations should conduct a risk assessment.
Is there a duplication of incident notification between OVIC and DPC Cyber Incident Response Service (CIRS)?	No, there are some differences between the two. Notification to OVIC relates to: • organisations to which Part 4 of the PDP Act applies, and • all information regardless or format i.e. hard copy, electronic, verbal. Notification to CIRS relates to: • cyber (electronic information) incidents, and • any VPS organisation who requires incident **response** assistance. OVIC and CIRS is in the process of developing a Memorandum of Understanding (MOU) to enable the sharing of incident information where possible to minimise the reporting burden of organisations.

Question/Comment	OVIC response
What is considered 'significant change'?	Refer to the VPDSF Glossary. A substantial change to the organisation's operating environment e.g. new functional business unit added/removed impacting on the type of information that the organisation handles, changes to the threat landscape impacting on the organisation's identified information risks.
At what level should security clearances start?	A requirement for a security clearance is based on the: • business impact level (BIL) of the resources the individual requires access to; and /or • the level of assurance required from the position by the organisation. Personnel with ongoing access to security classified information i.e. PROTECTED and above should hold a security clearance. A security clearance does not negate the 'need to know'.
What does element *'X'* mean?	Examples have been provided in brackets throughout the elements to clarify the intent of some of these. Further detail regarding implementing each of the elements is available in the primary sources listed alongside each of the elements.

Further Information

Contact Us

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