Office of the Victorian Information Commissioner

Information Security Team

Protective Data Security Plan

Victorian Protective Data Security Standards

Reporting information security capability and implementation progress

August 2020

Table of Contents

Document details

Version	Publish date	Amendments in this version
1.0	Sep 2017	Original (Excel spreadsheet)
1.1	Feb 2018	• High Level Protective Data Security Plan (Word document) replaced. • Renamed the original protective data security plan to detailed protective data security plan • Reporting by exception.

1.2	TBA	• For formal reporting purposes, this version of the PDSP replaces
		  ○ High Level PDSP
		  ○ Detailed PDSP
		  ○ Self-Assessment
		• Added the following components to the PDSP
		  ○ Executive Summary
		  ▪ Highlights from the past 24 months
		  ▪ Challenges and Barriers
		  ○ Information Security Self-assessment
		  ○ Organisation Profile Assessment
		  ○ Feedback to OVIC
		• Attestation is now a single artefact attached to this document.

Introduction to the Protective Data Security Plan

This Protective Data Security Plan (PDSP) is designed to help you assess your organisation's information security capability, summarize your progress towards your implementation of the Victorian Protective Data Security Standards (Standards), and for the Office of the Victorian Information Commissioner (OVIC) to assess Victorian's agencies and bodies progress to improving information security.

To achieve this, your report should have enough detail to understand the progress that you have made in information security capability and capture any issues and barriers that you have identified.

The PDSP is a useful document for you to validate the capability uplift journey you are on and confirm that activities are in place to achieve your desired level of maturity over the next 24 months. The information captured in this document may provide a useful summary to key stakeholders within your agency to provide a level of confidence in how you are progressing against the implementation of the Standards.

This report includes four parts:

- Part A - An Agency Head (or equivalent) executive summary
- Part B - Reporting capability and implementation progress
- Part C - Gathering your feedback
- Part D - Attestation

How information will be used

The Office of the Victorian Information Commissioner has a responsibility to provide ministers and the public with assurance regarding information security capabilities across government. The information you provide in this report will be used as an input in determining progress towards meeting information security objectives that will form the basis of reporting to you and the Victorian Government.

The OVIC Information Security team will:

- use self-assessment reports to help plan its engagement and support work
- use information to inform assurance activities
- provide feedback to organisations based on the submissions
- use feedback provided for statistical reporting and for the improvement of our resources

The information you provide will be handled according to the classification you assign.

The contents of this Protective Data Security Plan are exempt from the Freedom of Information Act 1982.

More information

Contact the OVIC team at security@ovic.vic.gov.au if you would like more guidance on the assurance reporting process.

Part A - Agency Head executive summary

Name of public sector agency or body (Organisation)	<Organisation Name>	
Name of Organisation Head (e.g. Department Secretary, CEO)	Full name	<Full Name>
	Phone number	<Contact Number>
	Email address	<Email Address>
	Postal address	<Postal Address>
Name of person authorised by the Organisation Head to submit a copy of the high level PDSP (including attestation) (Only complete this section if the details are not the same as the public sector body Head provided above)	Full Name	<Full Name>
	Position Title	<Full Name>
	Phone number	<Contact Number>
	Email address	<Email Address>
	Postal address	<Postal Address>
Nominated point of contact (Information Security Lead) (Only complete this section if the details are not the same as the authorised person listed above)	Full Name	<Full Name>
	Position Title	<Full Name>
	Phone number	<Contact Number>
	Email address	<Email Address>
	Postal address	<Postal Address>

Name of portfolio agency in which the organisation operates	<Select a Portfolio>

Highlights from the past 24 months

[Note any significant milestones you have achieved in building security capability over the last year]

Challenges and barriers

[Identify any standards that you have been unable to progress as planned, and the barriers you have in achieving the expected outcomes.]

Organisation Profile Assessment

This section assists OVIC's understanding of your organisation's security profile.

Factors		Number
Number of Staff[1]		0
Does your organisation have **critical assets**[2]?		<Please enter>
Does your organisation obtain, generate, receive or hold information at Business Impact Level **(BIL) 2**[3] or higher?		<Please enter>
What is the protective marking[4] breakdown of information assets within your organisation?		**Approximate Percentage (%)**
	Official	0
	Official: Sensitive	0
	Protected	0
	Secret	0
	Top Secret	0
	Total Information Assets	**0**[5]
What were the number of **recorded** Information Security incidents[6] during this reporting period?		0
Third Party Arrangements	How many third-party arrangements with direct access to your information are in place?	0
	What is the highest value (BIL) of your information that the third parties are accessing?	1 - OFFICIAL
In which part of your organisation does the ongoing management of your information security program reside?		Corporate

[1] This will assist OVIC engagement activities
[2] Essential or important assets, which if severely compromised, degraded, rendered unavailable for an extended period or destroyed, would significantly impact on the social or economic wellbeing of the organisation or Victorian community.
[3] Business Impact Levels are described in OVIC's VPDSF Information Security Management Collection which can be found on our website www.ovic.vic.gov.au.
[4] Protective markings are described in OVIC's VPDSF Information Security Management Collection which can be found on our website www.ovic.vic.gov.au.
[5] Please note this is a calculated field and should add up to 100%. There is no error checking at this stage.
[6] Any information security incidents, not just ICT

Part B - Information security self-assessment and implementation plan

Instructions

Each Standard has several fields to complete. For an explanation of the form fields, please refer to Appendix A.

For the purpose of this draft Protective Data Security Plan, we include one sample standard. The final PDPSP will include all the standards.

Standard 1 – Information Security Management Framework

An organisation must establish, implement and maintain an information security management framework relevant to their size, resources and risk posture.

Maturity assessment

Current	2020 Target	Goal
<Select>	<Select>	<Select>

Element assessment

Elements	Applicable	Supporting Control library[7]	Implementation			Risk Ref	Comments
			Status	Associated Project, Program or BAU	Year		
001 Organisations have a documented, contextual information security management framework covering governance arrangements and the security domains of information, personnel, ICT and physical.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		
002 The information security management framework contains and references all legislative and regulatory drivers.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		
003 Organisations monitor information security compliance obligations and identify performance indicators.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		
004 Executive have defined information security functions, roles, responsibilities, competencies and authorities.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		
005 Organisations refer to the risk management framework in the information security management framework.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		
006 Executive have committed to providing sufficient resources to support information security.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		
007 The information security management framework is sufficiently communicated and accessible.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		
008 Executive have established and communicated an information security strategy and implementation plan.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		

[7] The control library reflects control library we expect the organisation to be sourcing. If an alternative control library is being used, please identify the dominate source - .this source should be functionally equivalent to the one indicated.

Elements	Applicable	Supporting Control library[7]	Implementation			Risk Ref	Comments
			Status	Associated Project, Program or BAU	Year		
009 Organisational information security documentation contains controls to manage risk.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		
010 Organisations monitor, review, validate and update the information security management framework.	Applicable	AS 27001:2015	Not Commenced		**2019/20**		

Part C - Feedback to OVIC (optional)

This step is optional and there is no obligation for this to be completed, however your feedback provides us with valuable insights into the value of the tools and advice we provide to organisations implementing the Victorian Protective Data Security Standards.

Area	Statement	1 Disagree	2 Mostly Disagree	3 Agree	4 Mostly Agree	5 Strongly Agree
Organisation Security practices	My organisations' staff and contractors understand the requirements of our internal security policies and procedures	☐	☐	☐	☐	☐
	My organisations' staff and contractors understand what security controls to apply when handling official information	☐	☐	☐	☐	☐
	My organisations' staff and contractors are able to identify and know how to report a security incident if one happens	☐	☐	☐	☐	☐
	My organisations' 3rd Parties, with direct access to my information, understands our organisations' internal security policies and procedures	☐	☐	☐	☐	☐
PDSP	The Protective Data Security Plan was easy to complete	☐	☐	☐	☐	☐
	I required external expertise/assistance to help complete the PDSP	☐	☐	☐	☐	☐
	The PDSP provides good oversight of our information security regime to our executives	☐	☐	☐	☐	☐
Resources	The VPDSF resources provide excellent information	☐	☐	☐	☐	☐
	Information security resources are easy to locate on the OVIC website	☐	☐	☐	☐	☐
	Specific information security communities of practices would be beneficial	☐	☐	☐	☐	☐
	VISN Forums are effective	☐	☐	☐	☐	☐
	OVIC should conduct more VISN forums in regional Victoria	☐	☐	☐	☐	☐
VPDSS	The VPDSS assist in addressing my organisations information security risks	☐	☐	☐	☐	☐
	The VPDSS are easy to understand	☐	☐	☐	☐	☐
	THE VPDSS scales well to meet the security needs of my environment	☐	☐	☐	☐	☐
	THE implementation of the VPDSS is seen as a risk-based activity rather than a compliance activity	☐	☐	☐	☐	☐
OVIC Information Security Team	Overall, the Information Security Team provide excellent service	☐	☐	☐	☐	☐
	The members of the information security team are seen as subject matter experts in their field	☐	☐	☐	☐	☐
	The information security team are responsive to your questions or concerns	☐	☐	☐	☐	☐

What else can we do to help?

[What additional support could we provide to help you achieve your information security goals over the next year?]

Would you be happy to have a conversation with a member of the OVIC Information Security Unit about your responses?	Yes ☐	No ☐

Part D - Attestation

Attestation

This attestation is submitted to the Information Commissioner in accordance with s 8D(2)(b) of the *Privacy and Data Protection Act 2014* and Standard 12 in the Victorian Protective Data Security Standards dated July 2016 (**the Standards**).

I, [name and position title], verify that [name of agency or body] has implemented the key activities or is in the process of implementing key activities (either in progress or planned), as required by the Standards, which are issued in accordance with s 86(1) of the *Privacy and Data Protection Act 2014* as part of the Victorian Protective Data Security Framework.

I am authorised by [name of agency or body] to make this attestation to the Information Commissioner.

Signed:

Print name:

Position:

Date:

Appendix A – Self-assessment and implementation plan form field explanations

Following is a description of the field, its purpose and list of possible values.

Maturity

The security measures identified in your self-assessment are a demonstration of the security capability in your organisation. The capability maturity model used in the VPDSF assists your organisation to assess the maturity of each standard appropriate to your security risks. Once these capabilities are identified, you can then measure the maturity of your organisation's security measures. These maturity levels should be used as a guide to help your organisation focus any improvement activities and security investment in maturing measures implemented to mitigate security risks. The nature of capability maturity models is such that not every organisation will need to achieve the highest maturity level in each of the elements. The maturity levels will be dependent on the economic, efficient and effective use of the resources available to your organisation. To help organisations contextualise these maturity levels, the following maturity descriptions are provided[8].

Value	Description
Informal	Processes are usually ad-hoc and undocumented. Some base practices may be performed within the organisation, however there is a lack of consistent planning and tracking. Most improvement activity occurs in reaction to incidents rather than proactively. Where practice is good it reflects the expertise and effort of individuals rather than institutional knowledge. There may be some confidence security-related activities are performed adequately, however this performance is variable and the loss of key staff may significantly impact capability and practice.
Basic	The importance of security is recognised and key responsibilities are explicitly assigned to positions. At least a base set of protective security measures are planned and tracked. Activities are more repeatable and results more consistent compared to the 'informal' level, at least within individual business units. Policies are probably well documented, but processes and procedures may not be. Security risks and requirements are occasionally reviewed. Corrective action is usually taken when significant problems are found.
Core	Policies, processes and standards are well defined and are actively and consistently followed across the organisation. Governance and management structures are in place. Risk assessment and management activities are regularly scheduled and completed. Historic performance information is periodically assessed and used to determine where improvements should be made.
Managed	Day-to-day activity adapts dynamically and automatically in response to situational changes. Quantitative performance measures are defined, baselined and applied to ensure security performance is analysed objectively and can be accurately predicted in advance. In addition to meeting VPDSS requirements, the organisation also implements many optional 'better practice' requirements in response to its risk assessment.

[8] Adapted from New Zealand Protective Security Requirements (PSR)

Optimised	Security is a strategic issue for the organisation. Long-term planning is in place and integrated with business planning to predict and prepare for protective security challenges. Effective continuous process improvement is operating, supported by real-time, metrics-based performance data. Mechanisms are also in place to encourage, develop and test innovations.

If your organisation has completed the 2018 or 2019 Self-assessment form, it may use the average of the individual element assessments to provide an overall maturity assessment for the standard.

Applicability

Completing this field will provide your organisation with its statement of applicability (SOA) with respect to the Standards. Review each of the elements listed and select either 'Yes' if it applies or 'No' if it does not.

As a general rule, most of the elements will apply and only a few may not, depending on your organisation's value assessments of its information assets e.g. elements related to specific topics [9]such as:

- PER-060 Organisations with roles handling security classified information or requiring high assurance develop security clearance policies and procedures
- PER-070 Organisations with roles handling security classified information or requiring high assurance undertake additional personnel screening measures commensurate with the risk

Value	Description
Yes	The requirement is applicable to the organisation and mitigates an identified risk
No	The requirement is not applicable to the organisation as there is NO identified risk

Control Library Used

The VPDSS Elements are a list of high-level outcomes and serve two purposes, to:

- modify risks
- be implemented in order to meet the objectives of the Standards

Whilst your organisation implements specific controls to treat risks, the corresponding security elements for these controls identify how your organisation is tracking with implementation of the Standards. This outlines the expectations for the consistent implementation of the Standards.

Each element has been derived from a particular control library, that provides further guidance on security measures to assist organisations in their implementation. These measures are what we would expect to see implemented, i.e. the default. However, some organisations have implemented control libraries that already mitigate risks - that at least have functional equiveillance in their application. As this is a risk-based approach, OVIC accepts alternative security measures that at least support the intent of the standard and modify your organisational risk.

When selecting security measures to treat risks, consider the most effective, efficient and economic use of your budget. The grouping of like risks, or risks from similar threats, even when they have different ratings, may allow you to achieve better value for money.

[9] VPDSS 1.1 -Standard 16, Personnel Security

Identify a range of security measures that when used singularly or in combination will allow you to treat the risks to an acceptable level. Additionally, when selecting a range of security measures, not all measures should be of a technical nature, and may also relate to processes and people. All measures should be considered.

Security measures should also provide 'defence-in-depth'. That is, a number of measures may provide overlapping risk treatment which can provide some surety if one measure fails.

Below is a list of popular control libraries that are in use:

Library[10]	Description	
VPDSSE	Victorian Protective Data Security Standard Element	For organisations that determine the element is descriptive and inclusive enough as a control.
ISM	Australian Government Information Security Manual	The Australian Government Information Manual is a suite of controls designed to help Government agencies apply a risk-based approach to protecting their information and ICT systems. It helps organisations use their risk management framework to protect information and systems from cyber threats. The cyber security guidelines within the ISM are based on the experience of the ACSC within ASD.
NIST	National Institute of Standards and Technology Cybersecurity Framework	This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk.
AS 27002 ISO/IEC 27002:2015	Information technology - Security techniques - Code of practice for information security controls	The ISO/IEC 27000-series comprises mutually supporting information security standards that together provide a globally recognised framework for best-practice information security management.
Customised	No descriptor	A customised suite of controls that may not fit any particular individual control library OR a blend of control libraries.
Other	No descriptor	A control library that is not listed, please identify in the comments field

Implementation - Status

This records an organisation's current implementation status against each Standard.

Value	Description

[10] This is not meant to be an exhaustive list and we can may extend the list prior to final publication.

None	You have not yet defined or planned the work needed to meet the requirement. Alternatively, you have started work but there are significant risks it cannot be completed.
Planned	You have a program of work in place that includes work to meet the requirement; and the plan is appropriately phased and resourced.
Partial	You have delivered some of the elements needed to meet the requirement. Remaining work is underway and progressing as planned.
Meets	You currently meet the requirement.

Implementation - Associated Project, Program or BAU

This field records the Project, Program or BAU activity that is linked to the VPDSS element or controls being implemented.

Implementation - Year

Please enter the expected financial year that the implementation of the VPDSS element is expected.

Risk Reference

Depending on the maturity of an organisation's risk management framework and processes, security risks will be managed in either the VPDSF SRPA template or an organisational risk register

The purpose of this field is to identify the organisational risk reference that the implemented control(s) address. For example, it is expected that an organisation has at least one information security risk registered and the purpose of implementing the controls is to treat this risk in a meaningful way. For further understanding of risk management please refer to Chapter One of OVIC's Assurance collection – Protective Data Security Risk Profile Assessment.

Risk Reference
Free text field for referencing risk(s) that the control is treating.