Office of the Victorian Information Commissioner

Protective Data SecurityPlan (PDSP)

Information Security

Victorian Protective DataSecurityStandards

Reporting information security capability and implementation progress

Single-Organisation Reporting Form

Version 3.5

This form is intended to be completed electronically.
Different software may preview form fields differently.

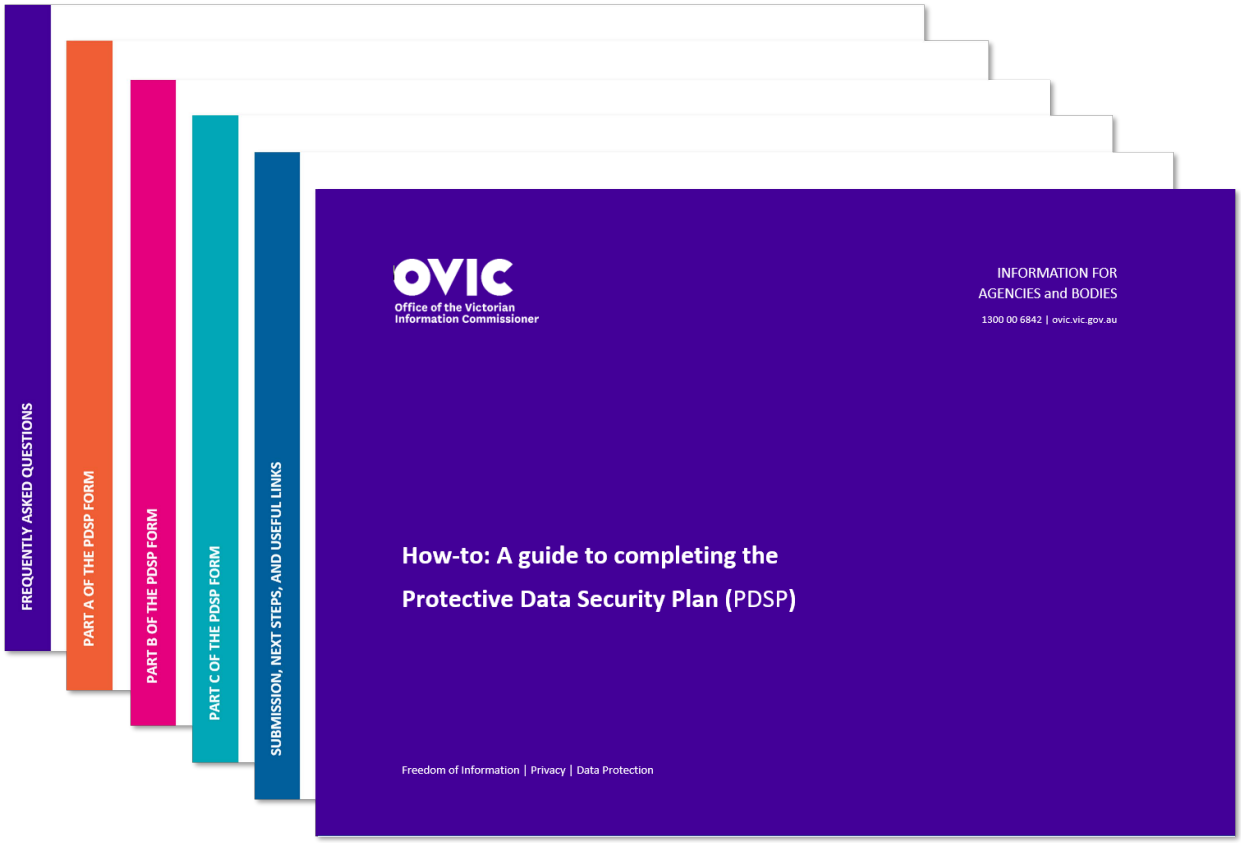
The 2024 PDSP form was developed using Acrobat 2020 (20.005.30467).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Table of Contents

Part A - Information security self-assessment and implementation plan

Instructions

Each Standard has a number of mandatory fields to complete. For an explanation of the form fields, please refer to the accompanying resource "**How to: A guide to completing the Protective Data Security Plan**" available from OVIC's website.



Note to auditors

The purpose of the VPDSS is to provide a set of criteria for the consistent application of risk-based practices to manage the security of Victorian government information. Elements are security measures that modify risk.

When auditing against this PDSP, auditors should consider how specific controls are implemented with regard to the organisation's internal and external context; the security value of information; and, any associated risks. Auditors should avoid viewing the implementation of the Elements as a compliance activity and instead focus on the risk management aspects.

Standard 1 – Information Security Management Framework

An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.

VPDSS Standard 1 Element Assessment

	VPDSS Standard 1 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.			Not Commenced	
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.			Not Commenced	
E1.030	The organisation's information security management framework aligns with its risk management framework.			Not Commenced	
E1.040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.			Not Commenced	
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.			Not Commenced	
E1.060	Executive management owns, endorses and sponsors the organisation's ongoing information security program(s) including the implementation plan.			Not Commenced	
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.			Not Commenced	
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).			Not Commenced	
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.			Not Commenced	

	VPDSS Standard 1 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E1.100	The organisation documents its internal control library that addresses its information security risks.			Not Commenced	
E1.110	The organisation monitors, reviews, validates and updates the information security management framework.			Not Commenced	
For those organisations that operate Industrial Automation and Control Systems (IACS) environments, fill in the following elements:					
E1.120	The organisation's information security framework defines the relationship between the business areas that support IT security and the business areas that support Industrial Automation and Control Systems (IACS) security.			Not Commenced	
E1.130	The organisation's information security framework differentiates security objectives of the Industrial Automation and Control Systems (IACS) from the enterprise systems.			Not Commenced	

VPDSS Standard 1 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 2 – Information Security Value

An organisation identifies and assesses the security value of public sector information.

VPDSS Standard 2 Element Assessment

	VPDSS Standard 2 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.			Not Commenced	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (**IAR**) in consultation with its stakeholders.			Not Commenced	
E2.030	The organisation uses a contextualised VPDSF business impact level (**BIL**) table to assess the security value of public sector information.			Not Commenced	
E2.040	The organisation identifies and documents the security attributes (confidentiality, integrity, and availability business impact levels) of its information assets in its information asset register.			Not Commenced	
E2.050	The organisation applies appropriate protective markings to information throughout its lifecycle.			Not Commenced	
E2.060	The organisation manages the aggregated (combined) security value of public sector information.			Not Commenced	
E2.070	The organisation continually reviews the security value of public sector information across the information lifecycle.			Not Commenced	
E2.080	The organisation manages externally generated information in accordance with the originator's instructions.			Not Commenced	
E2.090	The organisation manages the secure disposal (archiving/ destruction) of public sector information in accordance with its security value.			Not Commenced	

For those organisations that operate Industrial Automation and Control Systems (IACS) environments, fill in the following elements:		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E2.100	The organisation identifies, documents, and maintains the security attributes (confidentiality, integrity, and availability business impact levels) of its process automation assets in a register.			Not Commenced	

VPDSS Standard 2 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 3 – Information Security Risk Management

An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks.

VPDSS Standard 3 Element Assessment

	VPDSS Standard 3 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E3.010	The organisation conducts security risk assessments and determines treatment plans in accordance with its risk management framework covering all the processes to manage information security risks including: • Risk identification; • Risk analysis; • Risk evaluation; and, • Risk treatment			Not Commenced	
E3.020	The organisation records the results of information security risk assessments and treatment plans in its risk register.			Not Commenced	
E3.030	The organisation considers information security risks in organisational planning.			Not Commenced	
E3.040	The organisation communicates and consults with internal and external stakeholders during the information security risk management process.			Not Commenced	
E3.050	The organisation governs, monitors, reviews, and reports on information security risk (e.g., operational, tactical and strategic through a risk committee (or equivalent, e.g., audit, finance, board, corporate governance)).			Not Commenced	

VPDSS Standard 3 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 4 – Information Access

An organisation establishes, implements and maintains an access management process for controlling access to public sector information.

VPDSS Standard 4 Element Assessment

	VPDSS Standard 4 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E4.010	The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know.			Not Commenced	
E4.020	The organisation documents a process for managing identities and issuing secure credentials (registration and de-registration) for physical and logical access to public sector information.			Not Commenced	
E4.030	The organisation implements physical access controls (e.g., key management, swipe card access, visitor passes) based on the principles of least-privilege and need-to-know.			Not Commenced	
E4.040	The organisation implements logical access controls (e.g., network account, password, two-factor authentication) based on the principles of least-privilege and need-to-know			Not Commenced	
E4.050	The organisation manages the end-to-end lifecycle of access by following provisioning and de-provisioning processes.			Not Commenced	
E4.060	The organisation limits the use of, and actively manages, privileged physical and logical access and separates these from normal access (e.g., executive office access, server room access, administrator access).			Not Commenced	
E4.070	The organisation regularly reviews and adjusts physical and logical access rights taking into account operational changes.			Not Commenced	

VPDSS Standard 4 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 5 – Information Security Obligations

An organisation ensures all persons understand their responsibilities to protect public sector information.

VPDSS Standard 5 Element Assessment

	VPDSS Standard 5 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E5.010	The organisation documents its information security obligations and communicates these to all persons with access to public sector information (e.g., policies, position descriptions).			Not Commenced	
E5.020	The organisation's information security training and awareness content covers all security areas.			Not Commenced	
E5.030	The organisation delivers information security training and awareness to all persons with access to public sector information, upon engagement and at regular intervals thereafter in accordance with its training and awareness program and schedule.			Not Commenced	
E5.040	The organisation provides targeted information security training and awareness to persons in high-risk functions or who have specific security obligations (e.g., executives, executive assistants, procurement advisors, security practitioners, risk managers).			Not Commenced	
E5.050	The organisation reviews and updates the information security obligations of all persons with access to public sector information.			Not Commenced	
E5.060	All persons with access to public sector information acknowledge their information security obligations at least annually (e.g., during performance development discussions, attending security briefings, completing security training).			Not Commenced	
E5.070	The organisation monitors, reviews, validates, and updates its information security training and awareness program and schedule.			Not Commenced	

VPDSS Standard 5 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 6 – Information Security Incident Management

An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.

VPDSS Standard 6 Element Assessment

	VPDSS Standard 6 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E6.010	The organisation documents and communicates processes and plan(s) for information security incident management covering all security areas.			Not Commenced	
E6.020	The organisation articulates roles and responsibilities for information security incident management.			Not Commenced	
E6.030	The organisation's information security incident management processes and plan(s) contain the five phases of: · Plan and prepare; · Detect and report; · Assess and decide; · Respond (contain, eradicate, recover, notify); and, · Lessons learnt.			Not Commenced	
E6.040	The organisation records information security incidents in a register.			Not Commenced	
E6.050	The organisation's information security incident management procedures identify and categorise administrative (e.g., policy violation) incidents in contrast to criminal incidents (e.g., exfiltrating information to criminal associations) and investigative handover.			Not Commenced	
E6.060	The organisation regularly tests (e.g., annually) its incident response plan(s).			Not Commenced	

VPDSS Standard 6 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 7 – Information Security Aspects of Business Continuity and Disaster Recovery

An organisation embeds information security continuity in its business continuity and disaster recovery processes and plans. **VPDSS**

Standard 7 Element Assessment

	VPDSS Standard 7 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E7.010	The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas.			Not Commenced	
E7.020	The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans.			Not Commenced	
E7.030	The organisation regularly tests (e.g., annually) its business continuity and disaster recovery plan(s).			Not Commenced	

VPDSS Standard 7 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 8 – Third Party Arrangements

An organisation ensures that third parties securely collect, hold, manage, use, disclose or transfer public sector information.

VPDSS Standard 8 Element Assessment

	VPDSS Standard 8 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E8.010	The organisation's information security policies, procedures and controls cover the entire lifecycle of third party arrangements (e.g., contracts, MOUs and information sharing agreements).			Not Commenced	
E8.020	The organisation includes requirements from all security areas in third party arrangements (e.g., contracts, MOUs and information sharing agreements) in accordance with the security value of the public sector information.			Not Commenced	
E8.030	The organisation undertakes an information security risk assessment of the third party's service offering and addresses any residual risks prior to finalising the arrangement.			Not Commenced	
E8.040	The organisation identifies and assigns information security roles and responsibilities in third party arrangements (e.g., contracts, MOUs and information sharing agreements).			Not Commenced	
E8.050	The organisation establishes, maintains, and reviews a register of third party arrangements (e.g., contracts, MOUs and information sharing agreements).			Not Commenced	
E8.060	The organisation monitors, reviews, validates, and updates the information security requirements of third party arrangements and activities.			Not Commenced	
E8.070	The organisation documents its information release management requirements (e.g., social media, news, DataVic).			Not Commenced	
E8.080	The organisation manages the delivery of maintenance activities and repairs (e.g., on-site, and off-site).			Not Commenced	
E8.090	The organisation applies appropriate security controls upon completion or termination of a third party arrangement (e.g., contracts, MOUs and information sharing agreements).			Not Commenced	

VPDSS Standard 8 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 9 – Information Security Reporting to OVIC

An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (**VPDSS**) and reports to the Office of the Victorian Information Commissioner (**OVIC**).

VPDSS Standard 9 Element Assessment

	VPDSS Standard 9 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E9.010	The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level (**BIL**) of 2 (limited) or higher.	No response required. This is covered in the Attestation - Please refer to Part C of this PDSP form.			
E9.020	The organisation submits its Protective Data Security Plan (**PDSP**) to OVIC every two years.	No response required. This is implicit in the submission of this PDSP to OVIC.			
E9.030	Upon significant change, the organisation submits its reviewed PDSP to OVIC.	No response required. This is covered in the Attestation - Please refer to Part C of this PDSP form.			
E9.040	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.	No response required. This is covered in the Attestation - Please refer to Part C of this PDSP form.			

Standard 10 – Personnel Security

An organisation establishes, implements and maintains personnel security controls addressing all persons continuing eligibility and suitability to access public sector information.

VPDSS Standard 10 Element Assessment

	VPDSS Standard 10 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E10.010	The organisation's personnel security policies and procedures address the personnel lifecycle phases of: • Pre-engagement (eligibility and suitability); • Engagement (ongoing and re-engagement); and, • Separating (permanently or temporarily).			Not Commenced	
E10.020	The organisation verifies the identity of personnel, revalidates, and manages any changes as required.			Not Commenced	
E10.030	The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.			Not Commenced	
E10.040	The organisation manages ongoing personnel eligibility and suitability requirements commensurate with its security and probity obligations and risk profile.			Not Commenced	
E10.050	The organisation manages personnel separating from the organisation commensurate with its security and probity obligations and risk profile.			Not Commenced	
E10.060	The organisation develops security clearance policies and procedures to support roles requiring high assurance and/ or handling security classified information.			Not Commenced	
E10.070	The organisation undertakes additional personnel screening measures commensurate with the risk to support roles requiring high assurance and/ or handling security classified information.			Not Commenced	
E10.080	The organisation actively monitors and manages security clearance holders.			Not Commenced	

VPDSS Standard 10 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 11 – Information Communications Technology (ICT) Security

An organisation establishes, implements and maintains Information Communications Technology (**ICT**) security controls.

VPDSS Standard 11 Element Assessment

	VPDSS Standard 11 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E11.010	The organisation manages security documentation for its ICT systems (e.g., system security plans).			Not Commenced	
E11.020	The organisation manages all ICT assets (e.g., on-site, and off-site) throughout their lifecycle.			Not Commenced	
E11.030	The organisation conducts a security assessment for authorising systems to operate prior to transmitting, processing, or storing public sector information.			Not Commenced	
E11.040	The organisation undertakes risk-prioritised vulnerability management activities (e.g., patch management, penetration testing, continuous monitoring systems).			Not Commenced	
E11.050	The organisation documents and manages changes to ICT systems.			Not Commenced	
E11.060	The organisation manages communications security controls (e.g., cabling, telephony, radio, wireless networks).			Not Commenced	
E11.070	The organisation verifies the vendors security claims before implementing security technologies.			Not Commenced	
E11.080	The organisation manages security measures (e.g., classification, labelling, usage, sanitisation, destruction, disposal) for media.			Not Commenced	
E11.090	The organisation manages standard operating environments (**SOEs**) for all ICT assets, including end user access devices (e.g., workstations, mobile phones, laptops), network infrastructure, servers, and Internet of Things (**IoT**) commensurate with security risk.			Not Commenced	

	VPDSS Standard 11 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E11.100	The organisation manages security measures for email systems.			Not Commenced	
E11.110	The organisation logs system events and actively monitors these to detect potential security issues (e.g., intrusion detection/ prevention systems (**IDS/ IPS**)).			Not Commenced	
E11.120	The organisation uses secure system administration practices.			Not Commenced	
E11.130	The organisation designs and configures the ICT network in a secure manner (e.g., segmentation, segregation, traffic management, default accounts).			Not Commenced	
E11.140	The organisation manages a process for cryptographic keys (e.g., disk encryption, certificates).			Not Commenced	
E11.150	The organisation uses cryptographic controls for confidentiality, integrity, non-repudiation, and authentication commensurate with the risk to information.			Not Commenced	
E11.160	The organisation manages malware prevention and detection software for ICT systems.			Not Commenced	
E11.170	The organisation segregates emerging systems from production systems (e.g., physical and/ or logical) until their security controls are validated.			Not Commenced	
E11.180	The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing, retention).			Not Commenced	
E11.190	The organisation manages a secure development lifecycle covering all development activities (e.g., software, web-based applications, operational technology (Supervisory Control and Data Acquisition/ Industrial Control Systems (**SCADA/ICS**)).			Not Commenced	
E11.200	The organisation manages security measures for enterprise mobility (e.g., mobile device management, working from home).			Not Commenced	

VPDSS Standard 11 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Standard 12 – Physical Security

An organisation establishes, implements and maintains physical security controls addressing facilities, equipment and services.

VPDSS Standard 12 Element Assessment

	VPDSS Standard 12 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E12.010	The organisation plans and documents physical security measures.			Not Commenced	
E12.020	The organisation applies defence-in-depth physical security measures.			Not Commenced	
E12.030	The organisation selects physical security measures commensurate with the business impact level of the information.			Not Commenced	
E12.040	The organisation has scalable physical security measures ready for activation during increased threat situations.			Not Commenced	
E12.050	The organisation implements physical security measures when handling information out of the office.			Not Commenced	
E12.060	The organisation manages physical security measures throughout their lifecycle.			Not Commenced	

VPDSS Standard 12 Maturity Assessment

Current	2026 Target	2028 Aspiration

Use this space to provide any additional commentary 1500 character limit

- Supporting Control Library: Other
  If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable
  If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

Part B - Agency Head Executive Summary

Name of public sector agency or body

Public sector body Head (e.g., Department Secretary, CEO)	Full Name Position Title Phone Number Email Address Postal Address

Information Security Lead (The organisation's nominated contact regarding the VPDSS)	Full Name Position Title Phone Number Email Address Postal Address

In which part of the organisation does the ongoing management of the information security program reside?

Name of the Victorian government portfolio in which the organisation operates

Security program executive summary from the past 24 months Character limit 2,500

Challenges or barriers

Please select any challenges or barriers that may be inhibiting implementation of the Standards.

- ☐ Financial
- ☐ Resourcing
- ☐ Capability
- ☐ Legislative
- ☐ Significant change
- ☐ External third party dependencies
- ☐ Machinery of Government
- ☐ Lack of clarity around roles and responsibilities within the organisation
- ☐ Lack of understanding of the Standards
- ☐ Other

If relevant, please describe any challenges or barriers towards the implementation of the Standards Character limit 1,000

Organisation Profile Assessment

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

	Full-Time Equivalent	Contractors	Volunteers
Number of employees within the organisation			

Does the organisation have Industrial Automation and Control Systems (**IACS**)?
Does the organisation obtain, generate, receive or hold information at business impact level (**BIL**) 3 or higher?

Provide an approximate protective marking breakdown **(totaling 100%)** of the organisation's information assets:

BIL 1 (Confidentiality)	OFFICIAL	0	%
BIL 2 (Confidentiality)	OFFICIAL: Sensitive	0	%
BIL 3 (Confidentiality)	PROTECTED	0	%
BIL 3-4 (Confidentiality)	[security classification]// Cabinet-In-Confidence	0	%
BIL 4 (Confidentiality)	SECRET	0	%
BIL 5 (Confidentiality)	TOP SECRET	0	%
Percentage of information not assessed		0	%
Percentage of information marked using a former scheme or different scheme		0	%

Information Security Incidents	How many information security incidents were recorded in the organisation's internal incident register over the last 24 months?	
	Of these incidents, how many affected information assets of a BIL 2 or higher?	

Third Party Arrangements	How many third-party arrangements currently have direct access to the organisation's information and information systems?	
	What is the highest protective marking that third parties are accessing?	Unknown

How did the organisation validate the PDSP prior to submission to OVIC?

- Internal Audit ☐
- External Audit ☐
- Self-Assessed ☐

Additional comments (Optional) 300 character limit

Generative Artificial Intelligence

1. Does your organisation use Generative Artificial Intelligence (Gen AI)?

If you have selected *Planning* or *Yes:*

a. Nominate which tools are proposed or in use:

ChatGPT	☐	If 'Other', specify any additional tools. 300 character limit.
Google Gemini	☐	
Microsoft Copilot	☐	
Other	☐	

b. Select the types of public sector information proposed or in use as inputs into Large Language Models (LLMs) within your organisation.

Financial	Legal	Personal	Law Enforcement	Other	If 'Other', specify any additional types. 300 character limit.
☐	☐	☐	☐	☐	

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs within your organisation.

BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	Unknown
☐	☐	☐	☐	☐	☐

2. Do any of your Contracted Service Providers (CSPs) use Gen AI, in respect of public sector information collected, held, used, managed, disclosed or transferred on behalf of the organisation?

If you have selected *Planning* or *Yes:*

a. Nominate the Gen AI tools being proposed or in use by the CSP:

ChatGPT	☐	If 'Other', specify any additional tools. 300 character limit.
Google Gemini	☐	
Microsoft Copilot	☐	
Other	☐	

b. Select the types of public sector information proposed or in use as inputs into LLMs by the CSP.

Financial	Legal	Personal	Law Enforcement	Other	If 'Other', specify any additional types. 300 character limit.
☐	☐	☐	☐	☐	

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs by the CSP.

BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	Unknown
☐	☐	☐	☐	☐	☐

Part C - Attestation

Attestation

Under Part 4 of the *Privacy and Data Protection Act 2014* (PDP Act) and Standard 9 of the Victorian Protective Data Security Standards 2.0 (the Standards), I , attest that (E9.040) I am the public sector body Head of and my organisation:

- has undertaken, or is in the process of undertaking a security risk profile assessment (including assessment/s of any contracted service provider of my organisation, to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector information for my organisation) as required under section 89 of the PDP Act;

- ensures that a contracted service provider does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector information collected, held, used, managed, disclosed or transferred by the contracted service provider for my organisation;

- notifies the Office of the Victorian Information Commissioner of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information and systems with a business impact level (BIL) of 2 (limited) or higher (E9.010);

- has implemented the key activities, or is in the process of planning and implementing key activities, as required by the Standards; and

- upon significant change, submits a reviewed PDSP to the Office of the Victorian Information Commissioner (E9.030)

Print name:

Position:

Date:

Insert signature here