OVIC

Office of the Victorian
Information Commissioner

Protective Data Security Plan (PDSP)

Single organisation PDSP form

Version 3.7

Information Security

Victorian Protective Data Security Standards (VPDSS)

Reporting information security capability and implementation progress

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

The 2026 PDSP form was developed using Acrobat 2020 (20.005.30774).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Table of Contents

Information Security Obligations

Agencies and bodies subject to Part 4 of the *Privacy and Data Protection Act 2014* (VIC) (**PDP Act**) are responsible for protecting the information they generate, hold and manage and ensuring the right people have access to the right information at the right time. This includes securing systems that hold or transmit this information.

Part 4 PDP Act obligations

Section 88 of the PDP Act states that an agency or body must ensure that:

- it does not do an act or engage in a practice that contravenes a protective data security standard, in respect of —

    (a) public sector data collected, held, managed, used, disclosed or transferred by it; and
    (b) public sector data systems kept by it.

- any contracted service provider of the agency or body does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider for the agency or body.

Section 89 of the PDP Act states that within 2 years after the issue of protective data security standards applying to an agency or body—

- a security risk profile assessment
    - is undertaken for the agency or body, and
    - 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.
- a protective data security plan
    - is developed for the agency or body that addresses the protective data security standards applicable to that agency or body
    - must address compliance by any contracted service provider of the agency or body with the protective data security standards applicable to that agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body
    - is reviewed if there is a significant change in the operating environment or the security risks relevant to the agency or body.

- the public sector body Head for the agency or body must ensure that a copy of the protective data security plan is given to the Information Commissioner.

How will the information in the PDSP be used and managed?

In-line with OVIC's functions under the PDP Act, content from PDSP submissions may form the basis of reporting back to organisations and the Victorian Government including the Victorian Government Chief Information Security Officer.

OVIC will collect some personal information as part of the PDSP form including the name and contact details of the public sector body Head and nominated contact (Information Security Lead). OVIC will use this information to communicate with these contacts about the PDSP, broader security initiatives and activities, distributing information security-related content, or collecting feedback.

OVIC will not disclose personal information without consent, except where required to do so by law. For more information about how OVIC handles personal information, please see OVIC's Privacy Policy.

The information provided in the PDSP will be managed in accordance with the protective marking assigned. The contents of the PDSP are exempt from the *Freedom of Information Act 1982* (Vic).

Part A - Information security self-assessment and implementation plan

Instructions

Each Victorian Protective Data Security Standard (VPDSS or 'Standard') has a number of mandatory fields to complete. For an explanation of the form fields, please refer to the accompanying resource **"How-to Guide: Completing the Protective Data Security Plan (PDSP) 2026"** available on OVIC's website.

Introduction

How to use this guide

OVIC
Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES and BODIES
1300 00 6842 | ovic.vic.gov.au

How-to Guide: Completing the Protective Data Security Plan (PDSP)
2026

Freedom of Information | Privacy | Data Protection

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 this 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.

Standard 1 elementassessment

Standard 1 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation 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.				
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.				
E1.030	The organisation's information security management framework aligns with its risk management framework.				
E1.040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.				
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.				
E1.060	Executive management owns, endorses and sponsors the organisation's ongoing information security program(s) including the implementation plan.				
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.				
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).				
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.				

All fields on this page are mandatory unless otherwise stated

Standard 1 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E1.100	The organisation documents its internal control library that addresses its information security risks.				
E1.110	The organisation monitors, reviews, validates and updates the information security management framework.				

For those organisations that operate Industrial Automation and Control Systems (IACS) environments, fill in the following elements:

Standard 1 Industrial Automation Control Systems (IACS) elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
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.				
E1.130	The organisation's information security framework differentiates security objectives of the Industrial Automation and Control Systems (IACS) from the enterprise systems.				

All fields on this page are mandatory unless otherwise stated

Standard 1 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

Standard 2 - Information Security Value

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

Standard 2 element assessment

Standard 2 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.				
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.				
E2.030	The organisation uses a contextualised VPDSF business impact level (BIL) table to assess the security value of public sector information.				
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.				
E2.050	The organisation applies appropriate protective markings to information throughout its lifecycle.				
E2.060	The organisation manages the aggregated (combined) security value of public sector information.				
E2.070	The organisation continually reviews the security value of public sector information across the information lifecycle.				
E2.080	The organisation manages externally generated information in accordance with the originator’s instructions.				
E2.090	The organisation manages the secure disposal (archiving/ destruction) of public sector information in accordance with its security value.				

All fields on this page are mandatory unless otherwise stated

For those organisations that operate Industrial Automation and Control Systems (IACS) environments, fill in the following element:

	Standard 2 Industrial Automation Control Systems (IACS) elements	Entity Risk Reference(s)	Supporting Control Library	Implementation 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.				

Standard 2 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

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.

Standard 3 element assessment

	Standard 3 elements	Entity Risk Reference(s)	Supporting Control Library	Implementation 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				
E3.020	The organisation records the results of information security risk assessments and treatment plans in its risk register.				
E3.030	The organisation considers information security risks in organisational planning.				
E3.040	The organisation communicates and consults with internal and external stakeholders during the information security risk management process.				
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)).				

All fields on this page are mandatory unless otherwise stated

Standard 3 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

Standard 4 - Information Access

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

Standard 4 element assessment

	Standard 4 elements	Entity Risk Reference(s)	Supporting Control Library	Implementation 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.				
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.				
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.				
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.				
E4.050	The organisation manages the end-to-end lifecycle of access by following provisioning and deprovisioning processes.				
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).				
E4.070	The organisation regularly reviews and adjusts physical and logical access rights taking into account operational changes.				

All fields on this page are mandatory unless otherwise stated

Standard 4 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

Standard 5 - Information Security Obligations

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

Standard 5 element assessment

	Standard 5 elements	Entity Risk Reference(s)	Supporting Control Library	Implementation 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).				
E5.020	The organisation's information security training and awareness content covers all security areas.				
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.				
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).				
E5.050	The organisation reviews and updates the information security obligations of all persons with access to public sector information.				
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).				
E5.070	The organisation monitors, reviews, validates, and updates its information security training and awareness program and schedule.				

All fields on this page are mandatory unless otherwise stated

Standard 5 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

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.

Standard 6 element assessment

Standard 6 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation 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.				
E6.020	The organisation articulates roles and responsibilities for information security incident management.				
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.				
E6.040	The organisation records information security incidents in a register.				
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.				
E6.060	The organisation regularly tests (e.g., annually) its incident response plan(s).				

All fields on this page are mandatory unless otherwise stated

Standard 6 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

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.

Standard 7 element assessment

Standard 7 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E7.010	The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas.				
E7.020	The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans.				
E7.030	The organisation regularly tests (e.g., annually) its business continuity and disaster recovery plan(s).				

All fields on this page are mandatory unless otherwise stated

Standard 7 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

Standard 8 - Third Party Arrangements

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

Standard 8 element assessment

	Standard 8 elements	Entity Risk Reference(s)	Supporting Control Library	Implementation 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).				
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.				
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.				
E8.040	The organisation identifies and assigns information security roles and responsibilities in third-party arrangements (e.g., contracts, MOUs and information sharing agreements).				
E8.050	The organisation establishes, maintains, and reviews a register of third-party arrangements (e.g., contracts, MOUs and information sharing agreements).				
E8.060	The organisation monitors, reviews, validates, and updates the information security requirements of third-party arrangements and activities.				
E8.070	The organisation documents its information release management requirements (e.g., social media, news, DataVic).				
E8.080	The organisation manages the delivery of maintenance activities and repairs (e.g., on-site, and offsite).				
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).				

All fields on this page are mandatory unless otherwise stated

Standard 8 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

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**).

Standard 9 element assessment

	Standard 9 elements	Entity Risk Reference(s)	Supporting Control Library	Implementation 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.				
E9.020	The organisation submits its Protective Data Security Plan (PDSP) to OVIC every two years.		No response required.		
E9.030	Upon significant change, the organisation submits its reviewed PDSP to OVIC.		No response required.		
E9.040	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.		No response required.		

All fields on this page are mandatory unless otherwise stated

Standard 9 maturity assessment

Current	2028 Target	2030 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 10 - Personnel Security

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

Standard 10 element assessment

	Standard 10 elements	Entity Risk Reference(s)	Supporting Control Library	Implementation 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).				
E10.020	The organisation verifies the identity of personnel, revalidates, and manages any changes as required.				
E10.030	The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.				
E10.040	The organisation manages ongoing personnel eligibility and suitability requirements commensurate with its security and probity obligations and risk profile.				
E10.050	The organisation manages personnel separating from the organisation commensurate with its security and probity obligations and risk profile.				
E10.060	The organisation develops security clearance policies and procedures to support roles requiring high assurance and/ or handling security classified information.				
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.				
E10.080	The organisation actively monitors and manages security clearance holders.				

All fields on this page are mandatory unless otherwise stated

Standard 10 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

Standard 11 - Information Communications Technology (ICT) Security

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

Standard 11 element assessment

Standard 11 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E11.010	The organisation manages security documentation for its ICT systems (e.g., system security plans).				
E11.020	The organisation manages all ICT assets (e.g., on-site, and off-site) throughout their lifecycle.				
E11.030	The organisation conducts a security assessment for authorising systems to operate prior to transmitting, processing, or storing public sector information.				
E11.040	The organisation undertakes risk-prioritised vulnerability management activities (e.g., patch management, penetration testing, continuous monitoring systems).				
E11.050	The organisation documents and manages changes to ICT systems.				
E11.060	The organisation manages communications security controls (e.g., cabling, telephony, radio, wireless networks).				
E11.070	The organisation verifies the vendors security claims before implementing security technologies.				
E11.080	The organisation manages security measures (e.g., classification, labelling, usage, sanitisation, destruction, disposal) for media.				
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.				

All fields on this page are mandatory unless otherwise stated

Standard 11 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E11.100	The organisation manages security measures for email systems.				
E11.110	The organisation logs system events and actively monitors these to detect potential security issues (e.g., intrusion detection/ prevention systems (IDS/ IPS)).				
E11.120	The organisation uses secure system administration practices.				
E11.130	The organisation designs and configures the ICT network in a secure manner (e.g., segmentation, segregation, traffic management, default accounts).				
E11.140	The organisation manages a process for cryptographic keys (e.g., disk encryption, certificates).				
E11.150	The organisation uses cryptographic controls for confidentiality, integrity, non-repudiation, and authentication commensurate with the risk to information.				
E11.160	The organisation manages malware prevention and detection software for ICT systems.				
E11.170	The organisation segregates emerging systems from production systems (e.g., physical and/ or logical) until their security controls are validated.				
E11.180	The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing, retention).				
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)).				
E11.200	The organisation manages security measures for enterprise mobility (e.g., mobile device management, working from home).				

All fields on this page are mandatory unless otherwise stated

Standard 11 maturity assessment

Current	2028 Target	2030 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).

All fields on this page are mandatory unless otherwise stated

Standard 12 - Physical Security

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

Standard 12 element assessment

	Standard 12 elements	Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E12.010	The organisation plans and documents physical security measures.				
E12.020	The organisation applies defence-in-depth physical security measures.				
E12.030	The organisation selects physical security measures commensurate with the business impact level of the information.				
E12.040	The organisation has scalable physical security measures ready for activation during increased threat situations.				
E12.050	The organisation implements physical security measures when handling information out of the office.				
E12.060	The organisation manages physical security measures throughout their lifecycle.				

All fields on this page are mandatory unless otherwise stated

Standard 12 maturity assessment

Current	2028 Target	2030 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 - Organisation summary

Organisation information and contact details

Public sector agency or body

Name of the public sector agency or body	Preferred abbreviation of agency or body name (optional)

Organisation contacts

	Public sector body Head (e.g., Department Secretary, CEO)	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?

Specify if 'other' was selected

Name of the Victorian government portfolio in which the agency or body operates under.

Specify if 'other' was selected

If the 'Local Government' portfolio has been selected, nominate what information and system assets are covered by this PDSP.

(Multiple can be selected)

- □ Local Government Authority (Council) information and systems
- □ Committee of Management information and systems
- □ Class B Cemetery Trust information and systems

All fields on this page are mandatory unless otherwise stated

Provide an executive summary outlining the security program 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 changes
- □ Lack of clarity around roles and responsibilities within the organisation
- □ Lack of understanding of the Standards
- □ Other (specify below)

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

All fields on this page are mandatory unless otherwise stated

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			

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

Provide an approximate protective marking breakdown (totalling 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	%

Ensure the breakdown of the organisation's information assets equals **100%**

Information Security Incidents	How many information security incidents were recorded in the organisation's internal register over the last 24 months?	
	Of these incidents, how many affect information assets of a Business Impact Level (BIL) 2 or higher?	
Third-Party Arrangements	How many third-party arrangements currently have direct access to the organisation's information and systems?	
	What is the highest protective marking that third parties are accessing?	

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

Internal Audit □

External Audit □

Self-Assessed □

Additional comments (Optional) (300 character limit)

All fields on this page are mandatory unless otherwise stated

Shared service providers

1. Does your organisation currently provide shared services?

If *Yes* was selected, it is mandatory to complete sections *a* to *d*.

a) Nominate the number of services provided.

b) Nominate the number of entities your organisation provides services to.

c) Nominate the types of shared services provided by your organisation.

□ Audit
□ Communications/media
□ Corporate finance
□ Digital and analytics
□ Disposal
□ Fleet/asset management
□ Human Resources (HR)
□ Information Communication Technology (ICT)
□ Legal
□ Library
□ Payroll
□ Policy
□ Property/facilities/ accommodation
□ Records/information management
□ Unsure or other (specify below)

If 'Unsure' or 'Other', specify with detail
(500 character limit)

d) Is personal information involved in the provision of a shared service(s)?

2. Does your organisation currently receive shared services?

If *Yes* was selected, it is mandatory to complete sections *a* to *d*.

a) Nominate the number of services received.

b) Nominate the number of entities your organisation receives services from.

c) Nominate the types of shared services received by your organisation.

□ Audit
□ Communications/media
□ Corporate finance
□ Digital and analytics
□ Disposal
□ Fleet/asset management
□ Human Resources (HR)
□ Information Communication Technology (ICT)
□ Legal
□ Library
□ Payroll
□ Policy
□ Property/facilities/ accommodation
□ Records/information management
□ Unsure or other (specify below)

If 'Unsure' or 'Other', specify with detail
(500 character limit)

d) Is personal information involved in the provision of a shared service(s)?

Information security risks

As required under Part 4 of the *Privacy and Data Protection Act 2014* (Vic), organisations must undertake a Security Risk Profile Assessment (**SRPA**). This foundational process provides organisations insight into their information security risks which should be documented and managed via internal risk register(s).

For guidance on how to complete this mandatory section, refer to OVIC's *How-to Guide: Completing the Protective Data Security Plan*. A minimum of one risk reference and associated risk statement must be supplied to fulfill this section.

	Entity risk reference	Risk statement
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

All fields on this page are mandatory unless otherwise stated

Generative Artificial Intelligence

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

a. If *Planning* or *Yes,* please nominate which tools are proposed or in use:

ChatGPT □

Google Gemini □

Microsoft Copilot □

Other □

If 'Other', specify any additional tools (300 character limit)

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 Business Impact Level (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	BIL 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?

a. If *Planning* or *Yes,* please nominate which Gen AI tools being proposed or in use by the CSP:

ChatGPT □

Google Gemini □

Microsoft Copilot □

Other □

If 'Other', specify any additional tools (300 character limit)

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	BIL Unknown
□	□	□	□	□	□

All fields on this page are mandatory unless otherwise stated

Part C - Attestation

This Protective Data Security Plan (**PDSP**) is submitted to the Victorian Information Commissioner in accordance with section 89 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

I, *(full name)* as the public sector body Head of

(*organisation/agency/body*) confirm that:

- my organisation has implemented the 12 Victorian Protective Data Security Standards (**Standards**), or is in the process of planning and/or implementing these Standards (where applicable)
- the contents of this PDSP accurately reflect the current information security risks and program of my organisation, and
- I am aware of, and acknowledge, my obligations as public sector body Head as outlined under Part 4 of the PDP Act.

Print full name:

Position title:

Date:

Insert signature or sign here:

All fields on this page are mandatory unless otherwise stated