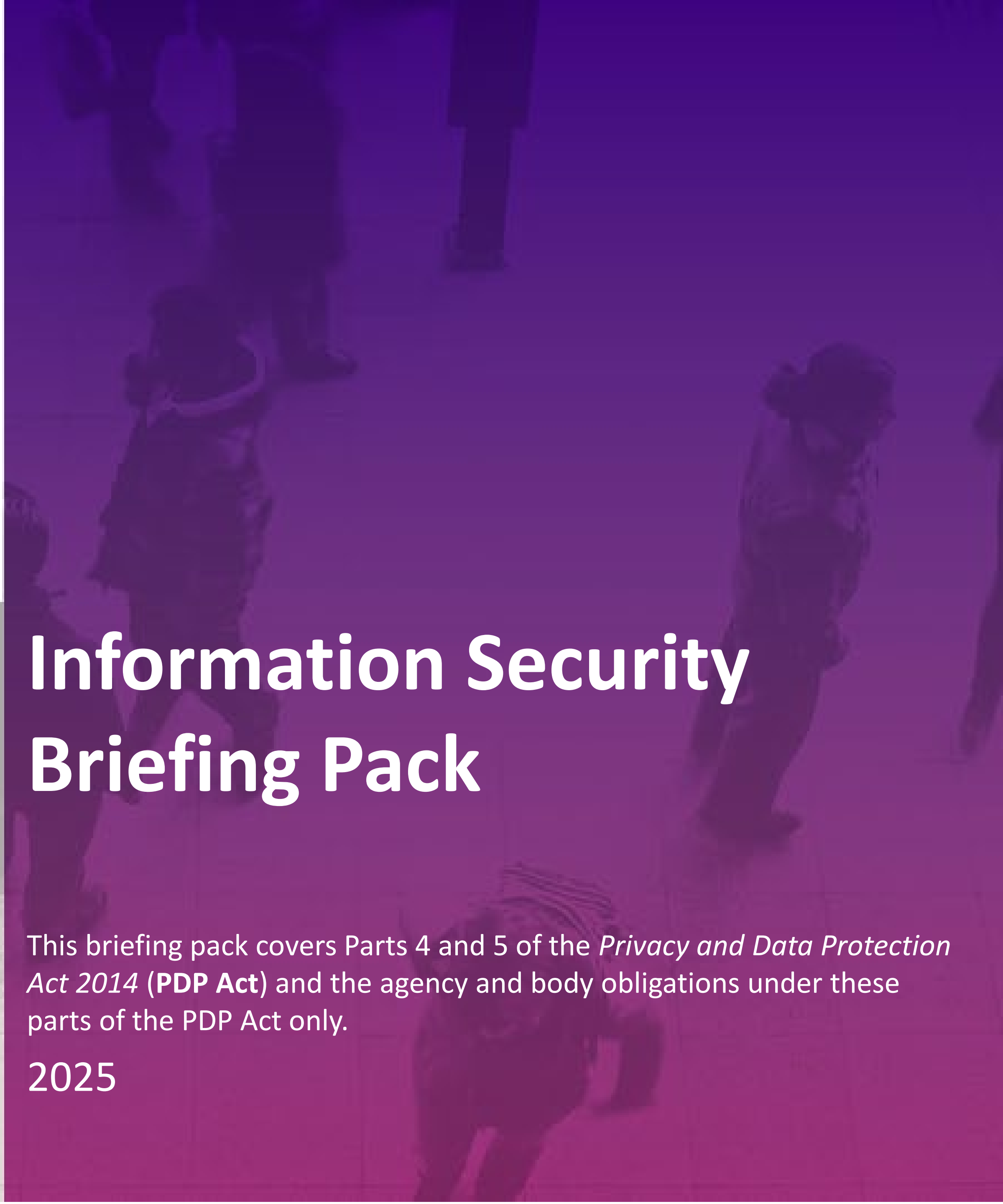
Office of the Victorian Information Commissioner



Information Security Briefing Pack

This briefing pack covers Parts 4 and 5 of the *Privacy and Data Protection Act 2014* (**PDP Act**) and the agency and body obligations under these parts of the PDP Act only.

2025

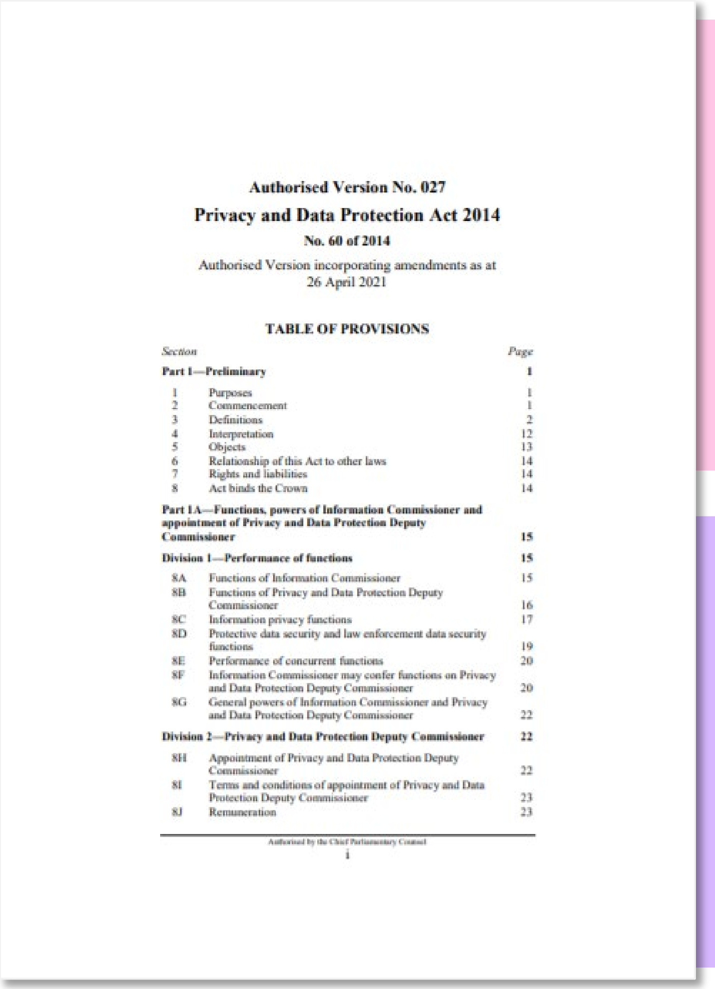
Contents

- The Privacy and Data Protection (**PDP**) Act 2014
  - What is public sector data (information)?
  - Who does Part 4 and 5 of the PDP Act apply to?
- The Victorian Protective Data Security Standards (**VPDSS**)
  - Implementation of the VPDSS
  - Information Security Domains / Areas: A Holistic Approach
- The Victorian Protective Data Security Framework (**VPDSF**)
  - Reporting to OVIC
- Implementation Approach
  - Five Step Action Plan
- Roles and Responsibilities
- Where to start

The Privacy and Data Protection (PDP) Act 2014

Parts 4 and 5 of the PDP Act detail the **information security requirements** applicable to:

- **Victorian government agencies and bodies (organisations)** and
- their **contracted service providers**.



Authorised Version No. 027

Privacy and Data Protection Act 2014

No. 60 of 2014

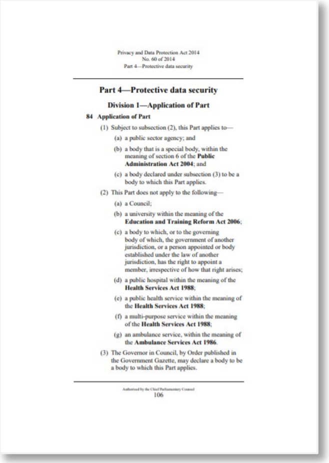
Authorised Version incorporating amendments as at
26 April 2021

TABLE OF PROVISIONS

Authorised by the Chief Parliamentary Counsel

i

Part 4



Privacy and Data Protection Act 2014
No. 60 of 2014
Part 4—Protective data security

Part 4—Protective data security

Division 1—Application of Part

84 Application of Part

(1) Subject to subsection (2), this Part applies to—

(a) a public sector agency; and

(b) a body that is a special body, within the meaning of section 6 of the **Public Administration Act 2004**; and

(c) a body declared under subsection (3) to be a body to which this Part applies.

(2) This Part does not apply to the following—

(a) a Council;

(b) a university within the meaning of the **Education and Training Reform Act 2006**;

(c) a body to which, or to the governing body of which, the government of another jurisdiction, or a person appointed or body established under the law of another jurisdiction, has the right to appoint a member, irrespective of how that right arises;

(d) a public hospital within the meaning of the **Health Services Act 1988**;

(e) a public health service within the meaning of the **Health Services Act 1988**;

(f) a multi-purpose service within the meaning of the **Health Services Act 1988**;

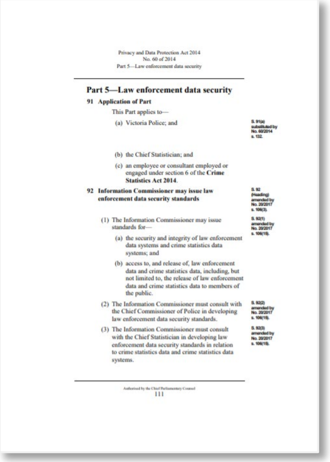
(g) an ambulance service, within the meaning of the **Ambulance Services Act 1986**.

(3) The Governor in Council, by Order published in the Government Gazette, may declare a body to be a body to which this Part applies.

Authorised by the Chief Parliamentary Counsel

106

Part 5



Privacy and Data Protection Act 2014
No. 60 of 2014
Part 5—Law enforcement data security

Part 5—Law enforcement data security

91 Application of Part

This Part applies to—

(a) Victoria Police; and

S. 91(a) substituted by No. 60/2014 s. 132.

(b) the Chief Statistician; and

(c) an employee or consultant employed or engaged under section 6 of the **Crime Statistics Act 2014**.

92 Information Commissioner may issue law enforcement data security standards

S. 92 (Heading) amended by No. 20/2017 s. 106(3).

(1) The Information Commissioner may issue standards for—

S. 92(1) amended by No. 20/2017 s. 106(15).

(a) the security and integrity of law enforcement data systems and crime statistics data systems; and

(b) access to, and release of, law enforcement data and crime statistics data, including, but not limited to, the release of law enforcement data and crime statistics data to members of the public.

(2) The Information Commissioner must consult with the Chief Commissioner of Police in developing law enforcement data security standards.

S. 92(2) amended by No. 20/2017 s. 106(15).

(3) The Information Commissioner must consult with the Chief Statistician in developing law enforcement data security standards in relation to crime statistics data and crime statistics data systems.

S. 92(3) amended by No. 20/2017 s. 106(15).

Authorised by the Chief Parliamentary Counsel

111

Link to the PDP Act:
https://www.legislation.vic.gov.au/in-force/acts/privacy-and-data-protection-act-2014/028

OVIC
Office of the Victorian Information Commissioner

What is public sector data (information)?

Public sector data is also referred to as **public sector information**.

This includes any information (including personal information) **obtained, generated, received** or **held** by or for a Victorian public sector organisation for an **official purpose** or supporting official activities.

It encompasses both **soft (electronic) and hard copy** information, regardless of media or format, as well as **verbal** information.

Who does Part 4 and 5 of the PDP Act apply to?

Organisations covered by Part 4 and 5 of the PDP Act include:

A public sector agency

A special body

A body as declared by the Governor in Council

Contracted service providers with direct and indirect access to public sector information

Victoria Police

Chief Statistician and personnel engaged under the *Crime Statistics Act 2014*

The Victorian Protective Data Security Standards (VPDSS)

What are they and what do they do?

- **12 high-level mandatory requirements** to protect public sector information across all security domains / areas
- Consistent with national and international standards that describe the **Victorian Government's approach to protecting public sector information**
- Focus on the outcomes that are required to **enable efficient, effective and economic investment** in security measures through a risk-managed approach

OVIC
Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards

Version 2.0

Freedom of Information | Privacy | Data Protection

ity Standards

Statement of Objective
To clearly establish, articulate, support and promote the security governance arrangements across the organisation and manage security risks to public sector information.
To ensure an organisation uses consistent identification and assessment criteria for public sector information across its lifecycle to maintain its confidentiality, integrity and availability.
To ensure an organisation manages information security risks through informed business decisions while applying controls to protect public sector information.
To formally authorise and manage the physical and logical access to public sector information.
To create and maintain a strong security culture by ensuring that all persons understand the importance of information security across all the security areas and their obligations for protecting public sector information.
To ensure a consistent approach for managing information security incidents, in order to minimise harm/damage to government operations, organisations or individuals.

3

Objective
organisation's revent, prepare, ge and recover from affects the , integrity and public sector
t the organisation's nformation is n the organisation a third party.
e organisation's ility and ensure king of its exposure to curity risks.
organisation's urity risks and provide pproach for managing h access to public tion.
secure environment by organisation's public tion through ICT ls.
secure environment by organisation's public tion through physical ls.

| Privacy | Data Protection 4

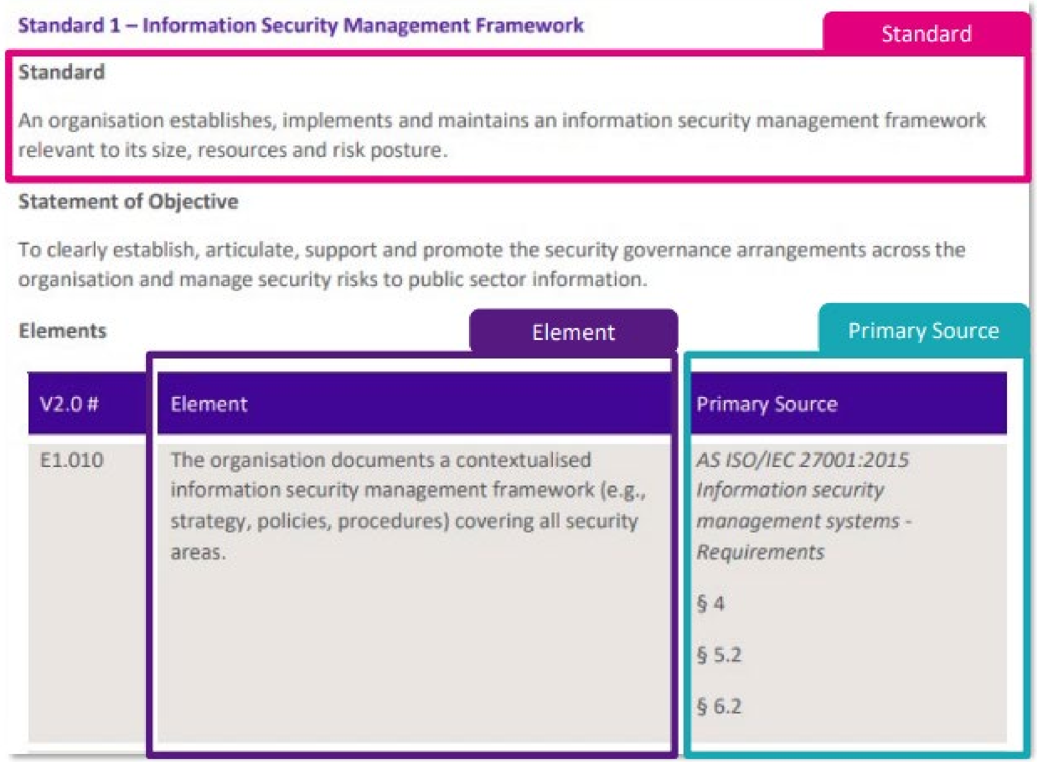
Link to the VPDSS
https://ovic.vic.gov.au/information-security/standards/

Implementation of the VPDSS

To assist organisations' adoption and implementation of the Standards, OVIC released the **VPDSS Implementation Guidance** which sets out each of the 12 Standards with a corresponding list of Elements (security measures).

Each Element is accompanied by primary source reference material that contains further detailed guidance on how to implement these measures.

Elements can assist organisations in protecting information assets based on the assessed security value and associated information security risks.



Standard 1 – Information Security Management Framework

Standard

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

Statement of Objective

To clearly establish, articulate, support and promote the security governance arrangements across the organisation and manage security risks to public sector information.

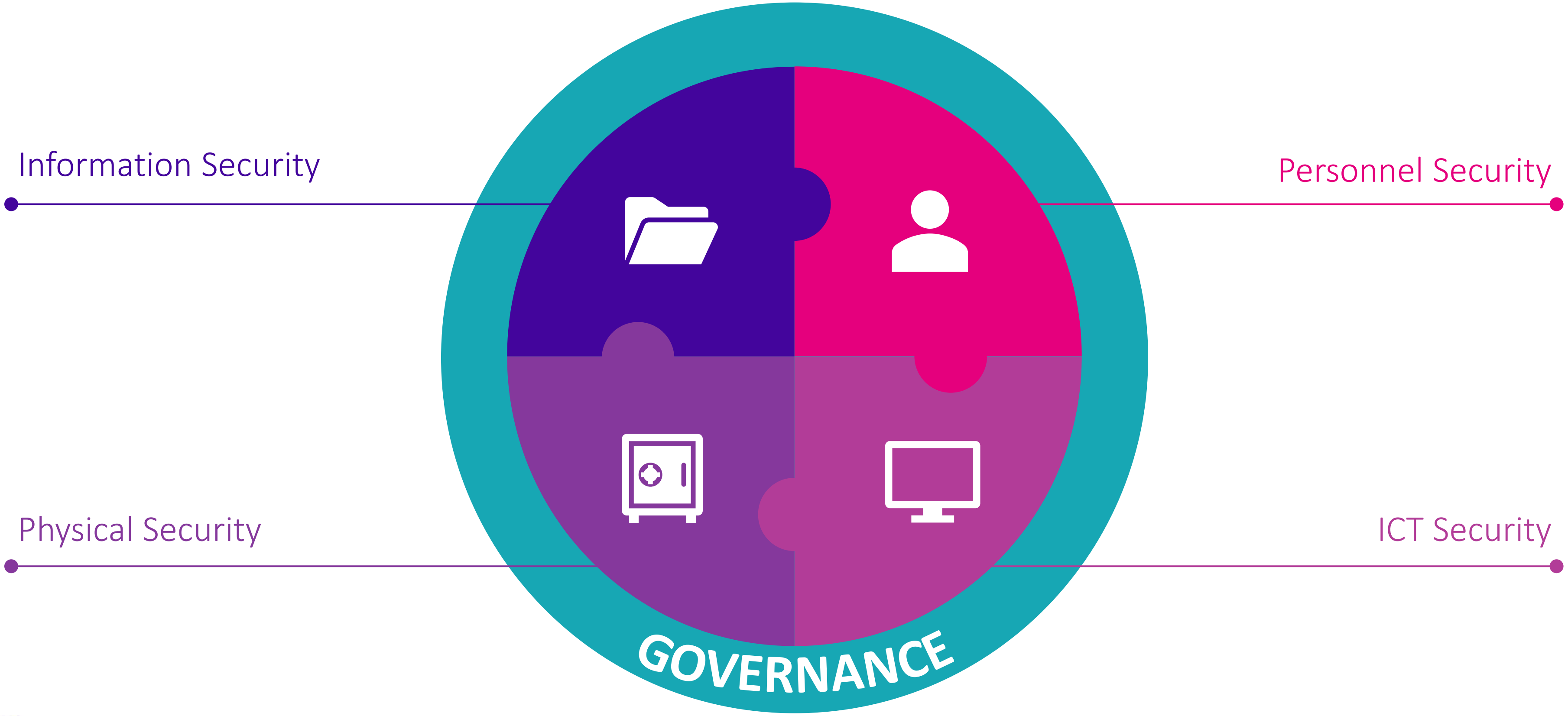
Elements

V2.0 #	Element	Primary Source
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.	*AS ISO/IEC 27001:2015 Information security management systems - Requirements* § 4 § 5.2 § 6.2

Link to the VPDSS Implementation
https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-standards-implementation-guidance/

Information Security Domains: A Holistic Approach

The Standards cover all aspects of the business -



Information Security

Personnel Security

Physical Security

ICT Security

GOVERNANCE

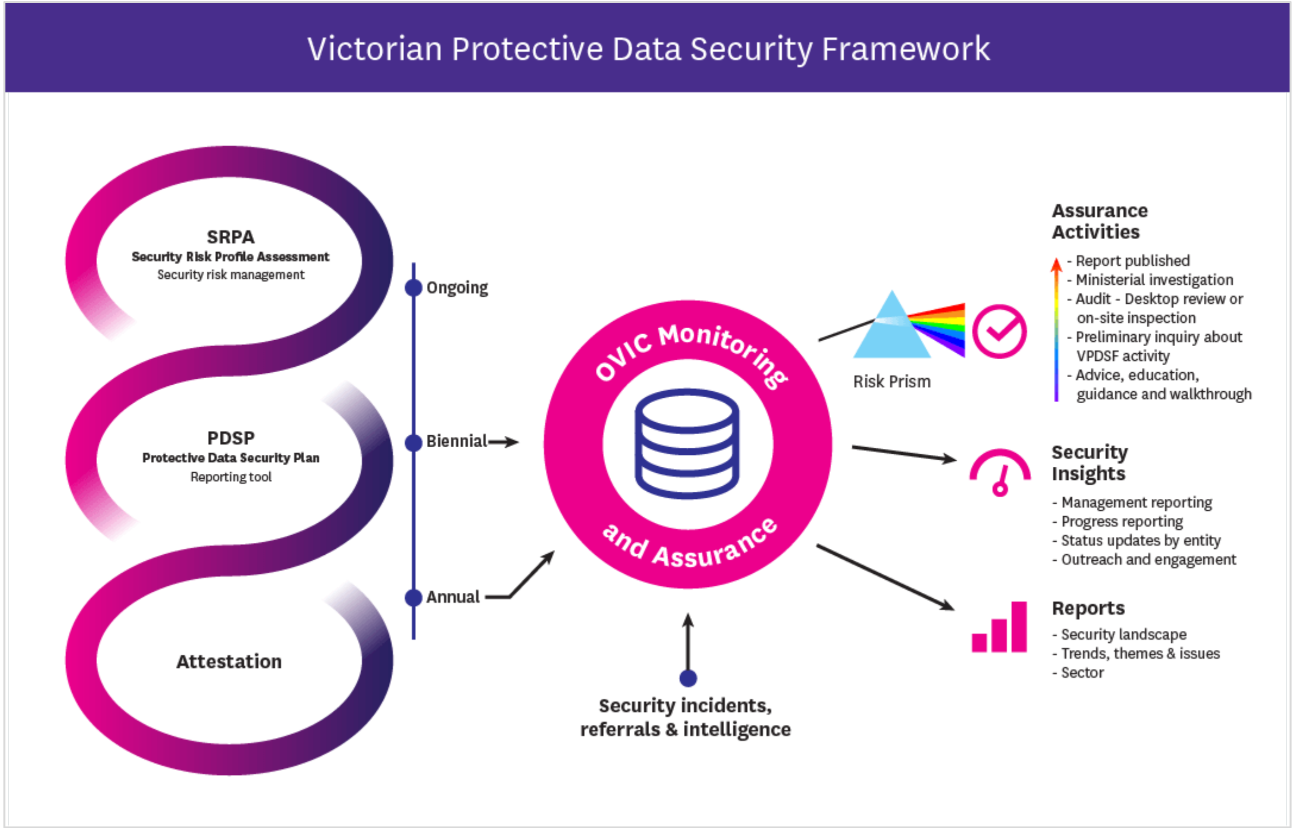
The Victorian Protective Data Security Framework (VPDSF)

What is the Framework?

Established under Part 4 of the PDP Act, the Framework has been developed to monitor and assure the security of public sector information, and information systems across the VPS.

The monitoring and assurance activities outlined in the Framework are based on:

- the compliance requirements of VPS organisations; and
- OVIC's responsibilities, powers and functions.


Victorian Protective Data Security Framework
SRPA
Security Risk Profile Assessment
Security risk management
PDSP
Protective Data Security Plan
Reporting tool
Attestation
Ongoing
Biennial
Annual
OVIC Monitoring and Assurance
Risk Prism
Security incidents, referrals & intelligence
Assurance Activities
- Report published
- Ministerial investigation
- Audit - Desktop review or on-site inspection
- Preliminary inquiry about VPDSF activity
- Advice, education, guidance and walkthrough
Security Insights
- Management reporting
- Progress reporting
- Status updates by entity
- Outreach and engagement
Reports
- Security landscape
- Trends, themes & issues
- Sector

Link to the VPDSF
https://ovic.vic.gov.au/data-protection/framework-vpdsf/

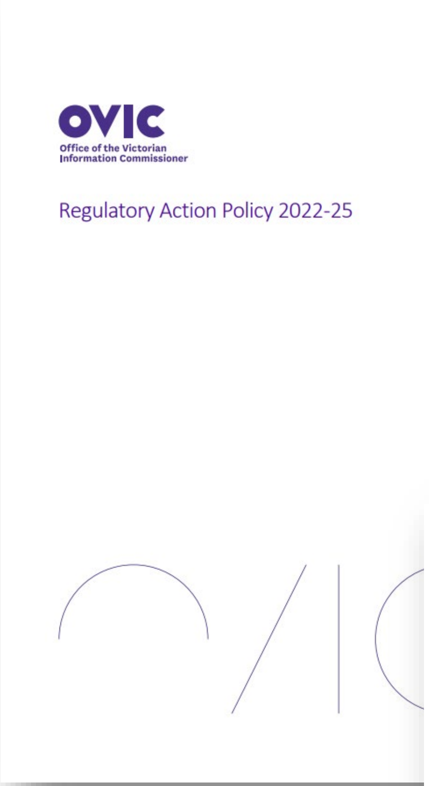
OVIC Regulatory Action Policy

What is the Regulatory Action Policy?

The Regulatory Action Policy explains how OVIC will use its powers.

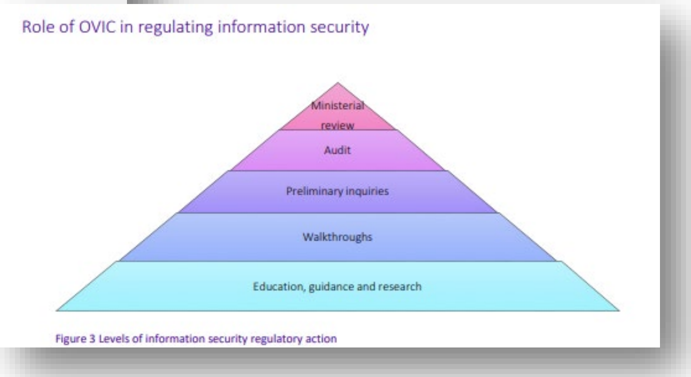
Our goal is to continue to instill in the Victorian public sector a culture that promotes fair public access to information while ensuring its proper use and protection. By doing so, we aim to build community trust in government handling of information.

The regulatory action that OVIC can take includes informal preliminary enquiries and engagement, audits and examinations, investigations, compliance notices and associated penalties as well as public reports.



OVIC
Office of the Victorian
Information Commissioner

Regulatory Action Policy 2022-25



Role of OVIC in regulating information security

Figure 3 Levels of information security regulatory action

Link to OVIC RAP
https://ovic.vic.gov.au/regulatory-action/regulatory-action-policy/

Key Activities and Reporting

Ongoing

Security Risk Profile Assessment (SRPA)

A SRPA is a process that enables VPS organisations to identify, analyse, evaluate and treat information security risks.

Biennial

Protective Data Security Plan (PDSP)

VPS organisations must **submit** a copy of its PDSP to OVIC every two years, or sooner in the event of significant change.

Annual

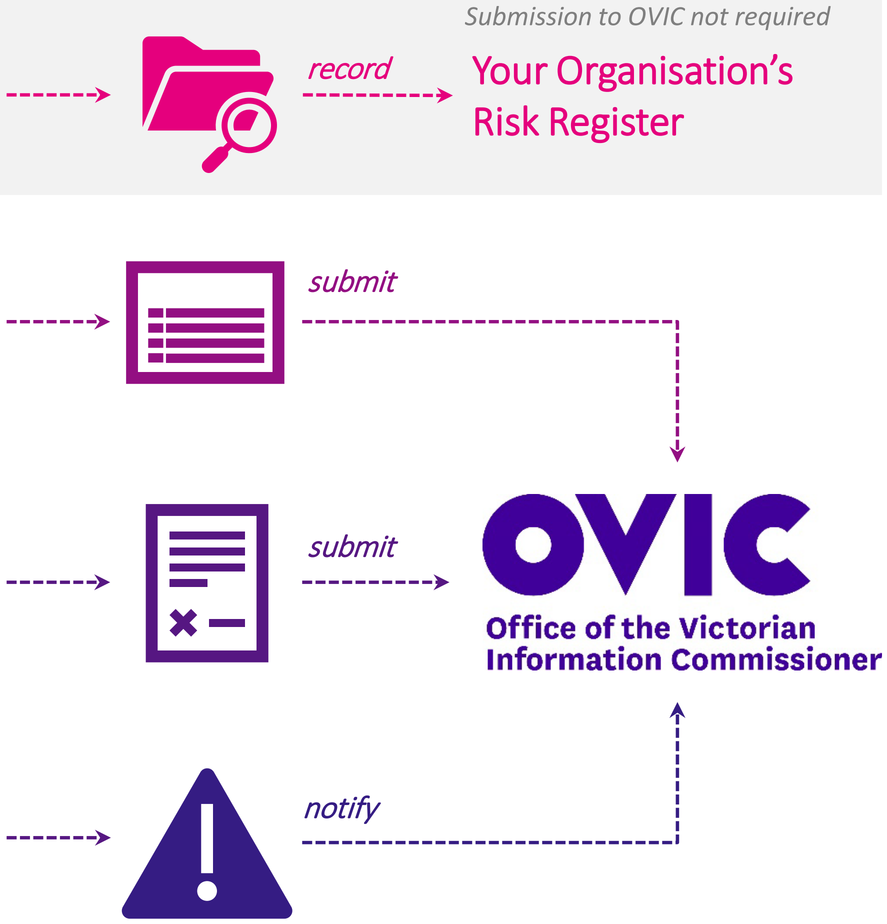
Attestation

VPS organisations must annually submit an Attestation on the progress of activities identified in its PDSP to OVIC.

Ongoing

Incident Notification

VPS organisations should **notify** OVIC of any information security incidents under the Security Incident Notification Scheme.



Submission to OVIC not required

record
Your Organisation's Risk Register
submit
submit
OVIC
Office of the Victorian Information Commissioner
notify

Link to Agency Reporting Obligations
https://ovic.vic.gov.au/information-security/agency-reporting-obligations/

Suggested Implementation Approach

Organisations may refer to the following steps when implementing the VPDSS -

1 Nominate an Executive Sponsor

An important first step includes the nomination of an **Executive Sponsor** who will champion the importance of information security throughout the business.

2 Establish an internal working group or body to coordinate efforts

To help focus efforts across the organisation, the Executive Sponsor may consider establishing a **working group** to help coordinate efforts in implementing the VPDSS. This group should **include representatives** from **all areas of the business**. This includes engaging representatives from:

- Governance areas
- Legal
- HR (People and Culture)
- Facilities
- Information/ Records Management
- ICT
- Finance, etc.

3 Confirm your organisation's Information Security Lead

While accountability for adhering to the VPDSS rests with the public sector body Head, they need to be supported by personnel who are appropriately skilled, resourced and empowered.

Your **information security lead** acts as a central point of contact for OVIC, helping deliver important information security messages and updates relating to the Framework and Standards.

Five Step Action Plan and Risk Management

	01	02	03	04	05
FIVE STEP ACTION PLAN	**Identify** your information assets	Determine the security ‘**value**’ of this information	Identify any **risks** to this information	**Apply** security measures to protect the information	**Manage** risks across the information lifecycle
RISK MANAGEMENT PROCESS	*Establish the overall information **risk context***		*Actively **addressing** risks*		***Ongoing** risk management*

Roles and Responsibilities

Public Sector Body Head

Under Part 4 of the PDP Act, public sector body Heads are ultimately accountable for adherence to the VPDSS and the monitoring and assurance activities of their organisation.

The public sector body Head is also required to seek their own form of assurance from any Contracted Service Provider / third party with access to the VPS organisation's public sector information and systems.

Information Security Lead (ISL)

Each public sector body Head must nominate an information security lead (**ISL**) for their organisation.

An organisation must notify OVIC of any changes to the lead, providing an alternative point of contact if they move roles or cease working for the organisation.

An ISL will:

- act as a central point of contact for OVIC
- deliver important information security messages and updates relating to the Framework and Standards
- help coordinate or guide the implementation of the Standards on behalf of the organisation

Link to Information Security Lead Info Sheet
https://ovic.vic.gov.au/data-protection/information-security-leads/

Where to start

Office of the Victorian Information Commissioner

01	02	03	04	05
Identify your information assets	Determine the **'value'** of this information	Identify any **risks** to this information	**Apply** security measures to protect the information	**Manage** risks across the information lifecycle

Information Security

The Five Step Action Plan

Victorian Protective Data Security Framework

Freedom of Information | Privacy | Data Protection

The **Five Step Action Plan** outlines practical activities designed to assist organisations manage information security risks.

Link: https://ovic.vic.gov.au/resource/the-five-step-action-plan/

Office of the Victorian Information Commissioner

INFORMATION FOR
AGENCIES

1300 00 6842 | ovic.vic.gov.au

Top Questions for the Audit and Risk Committee

A sense check guide to how the agency's VPDSF program is progressing

This document aims to provide Audit and Risk Committee (ARC) members with suggested questions to identify how the Victorian Protective Data Security Framework (VPDSF) uplift program is progressing and how commitments documented in the Protective Data Security Plan (PDSP) will be achieved.

Top Questions

1. "Have we developed a detailed project charter/work plan endorsed by the executive?"

Identify if the public sector organisation has developed and resourced an appropriate project/work plan to enable the systematic uplift of controls as per their PDSP. Determine if an appropriate level of project governance exists to ensure the project is meeting its objectives within budget and timelines.

2. "Is our progression against the work plan improving our information security maturity?"

Identify at a standards and controls level, where the public sector organisation has seen an uplift in maturity and by how much. How would this be demonstrated?

3. "If OVIC were to assess us today, how would we demonstrate our adherence to the VPDSF?"

Determine if the appropriate steps have been taken to understand the current state and develop an uplift plan (which should have been captured in the public sector organisation's detailed PDSP). These steps would have included:

- developing an Information Asset Register and populating with relevant information assets and their associated value
- identifying and assessing risks relevant to these assets into the Security Risk Profile Assessment
- developing a risk-based uplift in the Protective Data Security Plan, and
- undertaking the self-assessment against the Victorian Protective Data Security Standards

4. "Do we have a detailed internal control library and how aligned is it to the Victorian Protective Data Security Standards (VPDSS)?"

Determine if the organisation has identified and documented controls which demonstrate alignment to the VPDSS.

Freedom of Information | Privacy | Data Protection

lidation of these assets

date and any associated
ther work has taken place
vithin and outside of the
s / workshops) of the IAR

ich risk areas?"

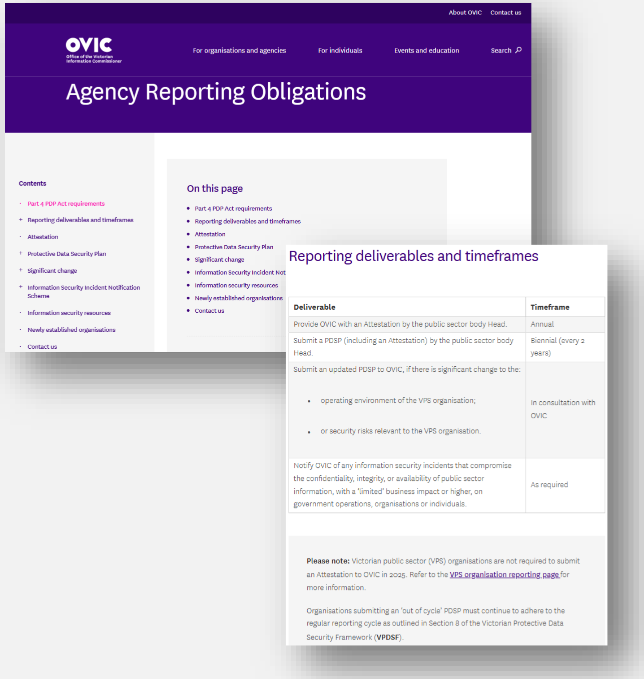
which controls were
as been achieved so far.
ppetite.

ed, and whether there is
internal audit). Determine
ls are assessed more
third parties and entities

ns of the Freedom of Information Act

This Info Sheet provides suggested questions to pose to an **Audit and Risk Committee** to understand how the organisation is managing its information security program.

Link: https://ovic.vic.gov.au/information-security/top-questions-for-the-audit-and-risk-committee/



About OVIC
Contact us
Office of the Victorian Information Commissioner
For organisations and agencies
For individuals
Events and education
Search

Agency Reporting Obligations

Contents

- Part 4 PDP Act requirements
- Reporting deliverables and timeframes
- Attestation
- Protective Data Security Plan
- Significant change
- Information Security Incident Notification Scheme
- Information security resources
- Newly established organisations
- Contact us

On this page

- Part 4 PDP Act requirements
- Reporting deliverables and timeframes
- Attestation
- Protective Data Security Plan
- Significant change
- Information Security Incident Not
- Information security resources
- Newly established organisations
- Contact us

Reporting deliverables and timeframes

Deliverable	Timeframe
Provide OVIC with an Attestation by the public sector body Head.	Annual
Submit a PDSP (including an Attestation) by the public sector body Head.	Biennial (every 2 years)
Submit an updated PDSP to OVIC, if there is significant change to the: • operating environment of the VPS organisation; • or security risks relevant to the VPS organisation.	In consultation with OVIC
Notify OVIC of any information security incidents that compromise the confidentiality, integrity, or availability of public sector information, with a 'limited' business impact or higher, on government operations, organisations or individuals.	As required

Please note: Victorian public sector (VPS) organisations are not required to submit an Attestation to OVIC in 2025. Refer to the VPS organisation reporting page for more information.

Organisations submitting an 'out of cycle' PDSP must continue to adhere to the regular reporting cycle as outlined in Section 8 of the Victorian Protective Data Security Framework (**VPDSF**).

Find out your agency's reporting obligations by visiting OVIC's **Agency Reporting Obligations** page.

Link: https://ovic.vic.gov.au/information-security/agency-reporting-obligations/

OVIC Information Security Video Series

Watch and share these videos to educate staff on information security matters and the importance of protecting public sector information and systems.

OVIC
Office of the Victorian Information Commissioner

INFORMATION SECURITY OVERVIEW

Watch this video to find out more about how information security safeguards public sector information.

OVIC
Office of the Victorian Information Commissioner

WHAT ARE THE VICTORIAN PROTECTIVE DATA SECURITY STANDARDS?

Watch this video to find out more about the VPDSS.

OVIC
Office of the Victorian Information Commissioner

WHICH ORGANISATIONS DOES PART 4 AND 5 OF THE PRIVACY AND DATA PROTECTION ACT APPLY TO?

Watch this video to find out which organisations Parts 4 and 5 apply to.

OVIC
Office of the Victorian Information Commissioner

WHAT ARE YOUR INFORMATION SECURITY RESPONSIBILITIES?

Information security is everyone's responsibility. Watch this video to found out how you can play your part in protecting public sector information.

Link to video series
https://ovic.vic.gov.au/information-security/information-security-videos/

OVIC
Office of the Victorian Information Commissioner

Contact the Information Security Unit for additional support and guidance.

security@ovic.vic.gov.au