Office of the Victorian Information Commissioner

Local Government Authorities (LGAs)

Information security obligations falling from Part 4 of the *Privacy and Data Protection Act 2014* (Vic)

2025

Table of contents

OVIC
Office of the Victorian Information Commissioner

A bit about OVIC

Who are we?

The Office of the Victorian Information Commissioner (**OVIC**) provides independent oversight of the Victorian public sector's collection, use and disclosure of public sector data (otherwise referred to as information) and systems.

The functions of OVIC are set out in two pieces of legislation –

- *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**)
    - **Part 3 -** Privacy
    - **Part 4 -** Data Protection
    - **Part 5 -** Law Enforcement Data Security
- *Freedom of Information Act 1982* (Vic) (**FOI Act**)

What we do

Under Part 4 of the PDP Act, the Information Commissioner has the power to:
- develop the Victorian Protective Data Security Framework and
- issue the Victorian Protective Data Security Standards (VPDSS or Standards).

These legislative instruments apply to most Victorian Public Sector (VPS) organisations.

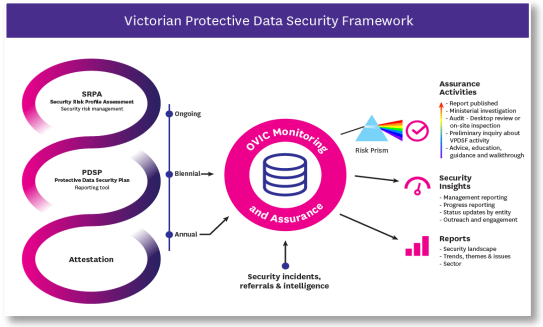
OVIC also conducts monitoring and assurance activities to gain insight into organisations adherence to the Standards. These assurance activities take the form of audits, reviews and/or investigations.

This pack focuses on Part 4 of the PDP Act, and the information security obligations of organisations captured by it.

The VPDSF and VPDSS

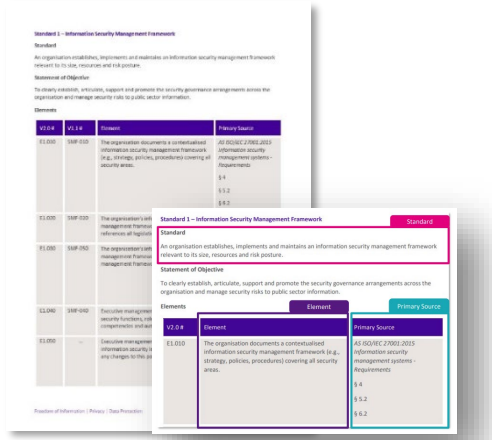
In summary, OVIC has developed and issued -

Victorian Protective Data Security Framework (**VPDSF**)



12 x Victorian Protective Data Security Standards (**VPDSS**)

98 x VPDSS Elements



These requirements inform the development of Council's **policies and procedures** as it relates to the protection of Council information and systems

What are the VPDSS?

Victorian Protective Data Security Standards

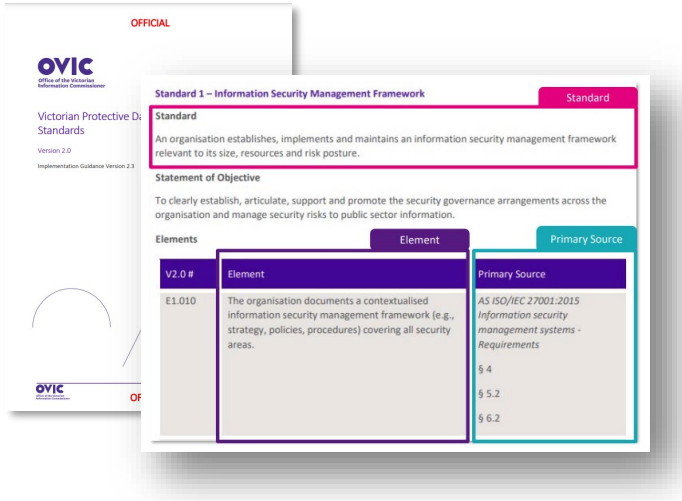
The VPDSS establish **high-level mandatory requirements** to protect public sector information and systems across all security domains/areas (e.g. Governance, Personnel, Physical, Cyber and Information security).

The Standards focus on the outcomes required to enable efficient, effective and economic investment in security measures through a risk-managed approach.

VPDSS - Implementation Guidance

The VPDSS is accompanied by Implementation Guidance. This guidance contains the **Standards** and **supporting Elements**.

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



What is covered by the VPDSS?

Information and systems governed by Part 4 of the PDP Act –

The PDP Act defines 'public sector data' and a 'public sector data system' as:

Public sector data

Any information (including personal information) obtained, received or held by an agency or body which Part 4 applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body;

…

The definition of public sector data includes information collected or held by contracted service providers of the VPS organisation who may be managing material on its behalf, including contractors and consultants.

Public sector data system(s)

Includes—

(a) information technology for storage of public sector data, including hardware and software; and

(b) non-electronic means for storage of public sector data; and

(c) procedures for dealing with public sector data, including by use of information technology and non-electronic means;

…

In summary, this means **any information and systems** obtained, received or held by an agency or body to which Part 4 of the PDP Act applies.

This includes both hard and soft copy information, regardless of media or format!

What is required?

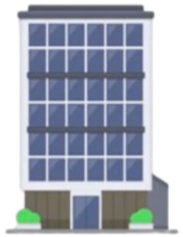
Under Part 4 of the PDP Act organisations must -

Broad requirements	PDP Act reference
Adhere to the VPDSS	Section 88 (1)
Ensure a Contracted Service Provider (**CSP**) adheres to the VPDSS	Section 88 (2)
Conduct risk assessments (Security Risk Profile Assessment – **SPRA**)	Section 89(1)(a)
Develop a treatment plan (**Protective Data Security Plan - PDSP**) to manage those risks	Section 89(1)(b)
Assess CSPs' risks	Section 89(2)
Ensure its PDSP addresses CSPs' compliance	Section 89(3)
Review the treatment plan (PDSP) every 2 years, or upon significant change	Section 89(4)
Submit a copy of the treatment plan (PDSP) to OVIC	Section 89(5)

Further, the VPDSS outline that organisations should -

Supplementary requirements	VPDSS Element
Attest annually to OVIC	E9.040
Notify 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	E9.010

Who is covered?



Public sector agency

Special body

Body declared by the Governor in Council

+

Contracted Service Provider(s)

Relevant sections of the PDP Act -

Sections 84 (1) and 84 (3)

Each of these entities are identified as 'applicable' **agencies** and **bodies** set out under Part 4 of the PDP Act (otherwise referred to as *regulated organisations*).

Section 88 (2)

A public sector body Head for an agency or a body to which this Part applies must ensure that a **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.

In this scenario public sector body Head of the regulated organisation maintains accountability for the maintenance of the confidentiality, integrity and availability of the public sector information.

LGA obligations

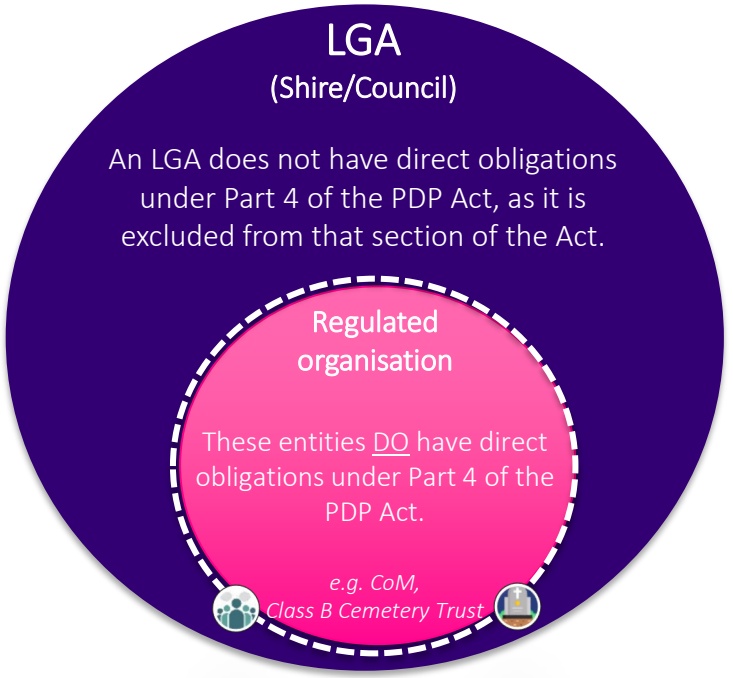
Part 4 PDP Act - Applicability

LGA (Shire/Council)

- Part 4 of the PDP Act references various agencies and bodies that are covered by the VPDSF and VPDSS. These are referred to as 'regulated organisations'.
- Part 4 of the PDP Act excludes LGAs; however, **this exclusion is limited** (i.e. only applies to the information and systems that relate to LGA functions).
- LGAs typically find themselves captured by Part 4 PDP Act where they undertake a function or activity of a regulated agency or body.
- In these instances, LGAs incur Part 4 PDP Act obligations of the entity, with respect to the information and systems they manage on its behalf.

Undertaking a function of a regulated organisation

- Regulated organisations that are captured under Part 4 of the PDP Act have obligations to securely manage their information and systems, as well as obligations to report to OVIC.
- Where an LGA undertakes a function or activity of a regulated organisation (e.g. Committee of Management or Class B Cemetery Trust) the LGA incurs Part 4 PDP Act obligations of that entity, with respect to the information and systems they manage on its behalf.
- As such, LGAs must abide by the conditions of Part 4 (including SRPA process and PDSP submission) as it relates to the information and systems of the regulated organisation.



NOTE! If a Council is unable to fully segment the information or systems of a regulated organisation from its broader information holdings, it must report on overall protective data security measures of the Council.

LGAs supporting a CoM and/or Class B Cemetery Trust

CoMs and/or Class B Cemetery Trusts applicability under Part 4 of the PDP Act -

Committees of Management (CoM)

A CoM is a public entity within the definition of Section 5 of the *Public Administration Act 2004* (Vic).

By this definition, CoMs must also adhere to the requirements of public entities under Part 4 of the PDP Act.

CoMs can be assigned to a Council where the public sector body Head of the Council takes responsibility for the CoM.

The appointed organisation who manages the CoM adopts the Part 4 PDP Act obligations of the CoM.

Class B Cemetery Trust (CT)

Class B Cemetery Trusts are considered public entities as they are established by the Governor in Council on the advice of the Minister as bodies corporate – per section 5 of the *Cemeteries and Crematoria Act 2003* (Vic).

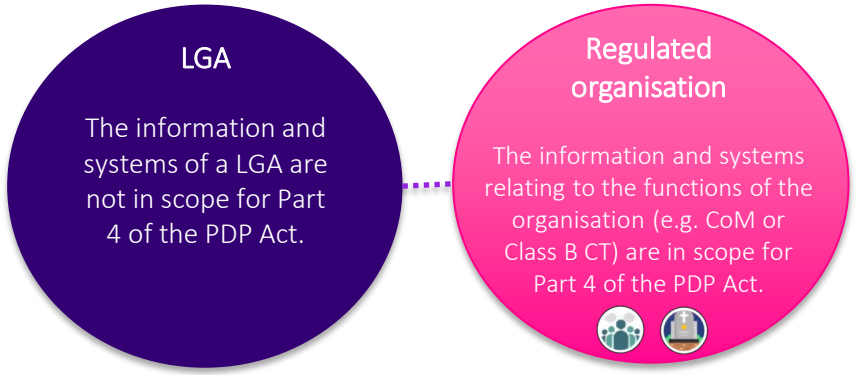
Where Councillors are appointed as trustees of a Class B CT, they and their staff working on Class B CT matters will be responsible for accessing, using and managing Class B CT information, and will use council systems to complete tasks.

As such, appointed personnel who manage Class B CT matters effectively adopt Part 4 PDP Act obligations of the CT.

NOTE! If an LGA is unable to fully segment the information or systems of a regulated organisation (e.g. CoM or CT) from its broader information holdings, the LGA must report to OVIC on the overall protective data security measures of the LGA.

Approaching the VPDSF and VPDSS as an LGA

Option 1 – Able to segment



In an ideal setting, an LGA would be able to separate its information holdings of the regulated organisation (e.g. CoM and/or Class B CT) from its broader information holdings.

In doing so, the requirements outlined in Part 4 of the PDP Act (inc. VPDSF and VPDSS) would be limited to the regulated organisation(s) and wouldn't consider the broader protective data security arrangements of the other information holdings of the LGA.

While Part 4 of the PDP Act requirements only relate to the regulated organisation, more often than not, the information and systems used to support the functions of the regulated organisation are managed by LGA personnel, stored within LGA facilities and processed / maintained using LGA systems / infrastructure.

Option 2 – Unable to segment

Often an LGA cannot fully segment the information and systems of a regulated organisation(s) from its broader information holdings. In these settings the security measures outlined under the VPDSS need to be applied to all information holdings of the Council.

Accompanying reporting obligations are also incurred by the Council per Part 4 of the PDP Act, including requirements set out in the VPDSF and the VPDSS.

OVIC
Office of the Victorian Information Commissioner

Proxy information security obligations

- Information Privacy Principles
- Information Sharing Arrangements
- Contractual Obligations
- Other legal and regulatory obligations

Overview of proxy obligations

There are a variety of scenarios where an organisation or individual (third-party) may incur information security obligations.

These can fall from:

Information Privacy Principles (IPPs)	Information Sharing Arrangements (incl. MOUs)	Other legal, regulatory and administrative requirements	Contractual obligations

Under Part 4 of the PDP Act, where a third-party -

- collects
- holds
- uses
- manages
- discloses or
- transfers

public sector information on behalf of a regulated organisation, the public sector body Head of the regulated organisation maintains accountability for the maintenance of the security of this material under the PDP Act.

Information Privacy Principles

Personal information – Part 3 of the PDP Act establishes legislative requirements to protect the privacy of individuals' information. It regulates the collection, handling and use of personal information in Victoria.

IPP4 – Data Security

- Under IPP 4.1 an organisation must take reasonable steps to protect the personal information it holds from misuse and loss, and from unauthorised access, modification or disclosure.

IPP 4.1 and Part 4 of the PDP Act support a risk-based approach to implementing security measures that are proportionate to their respective risks.

OVIC encourages organisations to apply the VPDSF and its Five Step Action Plan, as this complements the identification and implementation of security measures required under IPP 4.1.

For more information, please review the **IPP 4 – DATA SECURITY** guidance on OVIC's website by visiting https://go.vic.gov.au/3N3gOUX.

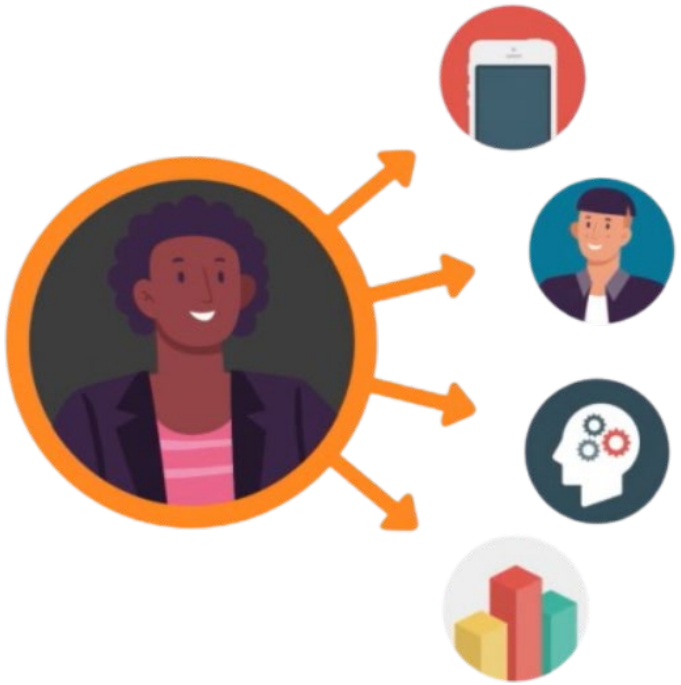
Information Sharing Arrangements

LGAs are party to a variety of information sharing arrangements, each with their own conditions.

These arrangements can take many forms, including Memoranda of Understanding (MOUs), Bilateral agreements, etc. Irrespective of their form, they often include information security provisions for organisations to comply with.

Provisions outlined in these agreements can vary – e.g. sometimes they describe detailed security controls, whereas other times there may be broad references to compliance with the PDP Act or VPDSS / VPDSF.

To help track these provisions, LGAs should establish a register of these information sharing arrangements. By doing so, LGA personnel will be better placed to monitor and understand what is required under the arrangement with respect to the information that is being accessed, used or managed.



Other legal and regulatory obligations

Like all organisations, LGAs have a raft of legal and regulatory obligations to cater to.

At times, these obligations may compel an LGA to provide a level of assurance around their information security practices, with many referring to OVIC's VPDSS as a primary source for how to implement this.

By way of example, the *Health Records Act 2001* (Vic) sets out conditions by which organisations are expected to maintain the privacy of an individual's health information.

Under HPP4.1 organisations must take **reasonable steps to protect the health information** it holds from misuse and loss and from unauthorised access, modification or disclosure.

For more information, please consider the advice offered on the Health Complaints Commissioner's website - https://hcc.vic.gov.au

Contractual obligations

Non-LGA organisations that are subject to Part 4 of the PDP Act, must ensure that contractual arrangements have the relevant information security requirements embedded into the terms or conditions of their agreements.

LGAs may find themselves subject to these contracts and must abide by the information security requirements outlined in these agreements. This may include providing assurance around the information security practices of the LGA.

The methods used, and extent to which a non-LGA regulated organisation may seek assurance will be influenced by the:

- security value of the information / system
- services or functions supported by the agreement and
- form of the arrangement.

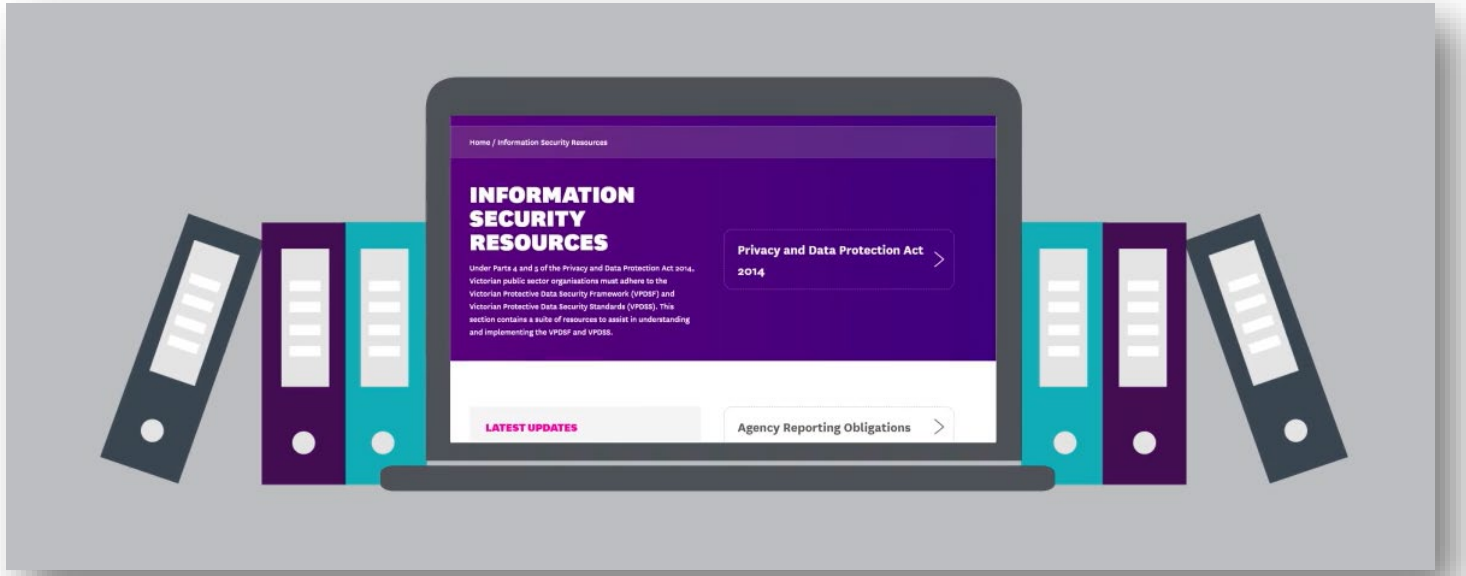
The assurance received from the LGA is a useful input into the non-LGA regulated organisation's SRPA process and development of their PDSP.

Benefits in implementing the VPDSS

An LGA:

- is better placed to identify and understand the security value of its information and system assets
- is well-positioned to achieve its business objectives in a secure manner
- (and its stakeholders) will have greater confidence in the information and systems that are relied upon to deliver key services and functions
- can provide a level of assurance to internal and external stakeholders around the information security practices across the business

Resources to assist you



Go to www.ovic.vic.gov.au to find out more, or reach out to the Information Security Unit by emailing security@ovic.vic.gov.au

OVIC