Office of the Victorian
Information Commissioner

DATA PROTECTION

Victorian Protective Data Security Framework

March 2018

Freedom of Information | Privacy | Data Protection

This page is intentionally left blank.

DATA PROTECTION

Victorian Protective Data Security Framework

March 2018

Published by the Office of the Victorian Information Commissioner
PO Box 24274
Melbourne Victoria 3001
Also published on:
https://www.ovic.vic.gov.au

VPDSF Document Details

Version	Publish Date	Amendments in this version
1.0	June 2016	NA
1.1	March 2018	• Change references of 'Commissioner for Privacy and Data Protection' to Office of the Victorian Information Commissioner' • Change references of 'CPDP' to OVIC' • Change references of 'PDPA' to 'PDP Act' • Replace 'Foreword' with new Deputy Commissioner's foreword • Insert new section on Victoria Police and the Crime Statistics Agency • Removed reference to annual security attestation in section 12 • Change 'protocol' descriptor • Insert reference to 'elements' • Insert reference to Part 5 – Assurance Model in section 17 for more information • Insert reference to Enterprise Solutions Branch in Section 19 • Remove 'sensitive and significant (valuable)' in section 20 • Updated some control references • Change Part 5 – Assurance Model – various including revised reporting obligations • Insert new section on single/multiple organisation reporting • Insert new section on the VPDSF 5-step action plan

This page is intentionally left blank.

Contents

Foreword

The Victorian Protective Data Security Framework (VPDSF) is the overall scheme for managing protective data security risks in Victoria's public sector. Established under Part Four of the Privacy and Data Protection Act 2014 (PDP Act), the framework consists of the:

- Victorian Protective Data Security Standards (the Standards)
- the Assurance Model
- supplementary security guides and supporting resources.

The VPDSF offers agencies and bodies a means to continually improve their information security practices, manage their risks, promote innovation and increase productivity. It encourages cultural change in the Victorian public sector by promoting information security as part of everyday business. Information security involves most areas of an organisation's activities, including people, buildings, systems and processes.

In June 2016 the Special Minister of State approved the Standards, which are based on national and international standards to integrate with existing efforts and investment in security. Adherence to the Standards became mandatory in June 2016 for public sector agencies and bodies, with some exclusions.

By applying the Standards, organisations are positioned to manage security risk more effectively and maintain a secure government operating environment. In this tightly-integrated world, a holistic approach to security is necessary.

The Assurance Model assists agencies and bodies to identify, analyse and evaluate their security risks more effectively. For this reason, the VPDSF requires that the public sector body head take responsibility for the assurance process.

The VPDSF Five Step Action Plan is strongly encouraged as an approach to implementing the VPDSF in a logical and staged manner. The protective data security obligations under the PDP Act require organisations to:

- undertake a detailed Security Risk Profile Assessment (SRPA)
- complete a VPDSF self-assessment (referencing the VPDSF Elements)
- develop a detailed Protective Data Security Plan (PDSP)
- review the PDSP at least every two years (or sooner if there is significant organisational change)

A high-level PDSP, including an attestation, must be submitted to OVIC by 31 August 2018, and every two years hereafter, or sooner if there is significant organisational change.

For the purposes of August 2018 reporting, organisations are to use the high level PDSP (and accompanying attestation) template for either single or multiple organisations. This reflects the Victorian public sector's unique operating requirements and diverse range of agencies and bodies. Some agencies have hundreds of smaller organisations within their portfolios, and not all those organisations are staffed well enough to undertake security activities on their own.

OVIC continues to develop supporting resources to assist agencies and bodies with implementation of the Standards. We will continue to develop and refine the VPDSF with the public sector, to achieve the most efficient, effective and economic delivery of Victorian Government business.

RACHEL DIXON
Privacy and Data Protection Deputy Commissioner
March 2018

This page is intentionally left blank.

Part One – Introduction

1. Privacy and Data Protection Act 2014

The *Privacy and Data Protection Act 2014* (PDP Act) significantly changes the regulatory landscape for data protection in the Victorian public sector.

Part Six of the PDP Act sets out the protective data security functions[1] of the Office of the Victorian Information Commissioner (OVIC), which are primarily to:

- develop the Victorian Protective Data Security Framework (VPDSF)
- issue the Victorian Protective Data Security Standards (VPDSS)
- establish a regime for monitoring and assuring public sector data security (Assurance Model).

2. Victorian Protective Data Security Framework

Established under Part Four of the PDP Act, the VPDSF provides direction to Victorian public sector agencies or bodies on their data security obligations. Reflecting the sector's unique operating requirements, it will build security risk management capability and maturity through the use of existing risk management principles and guidelines[2].

(In this document, agencies and bodies are referred to as organisations.)

3. Public sector data

Under the PDP Act, public sector data[3] means 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.

(In this document, public sector data is referred to as information.)

4. Protective data security

Protective data security is the practice of implementing security measures to protect Victorian government information.

Public sector organisations can achieve protective data security by:

- developing and documenting an Information Security Management Framework (ISMF) that satisfies governance and the four domains of protective data security: information, personnel, information communications technology (ICT) and physical security
- documenting security policies, standards and guidelines
- adopting a risk management framework
- identifying and implementing security measures.

[1] Privacy and Data Protection Act 2014, Part 6 – Division 2, s 103(2)

[2] Department of Treasury and Finance, *Victorian Government Risk Management Framework* (VGRMF), (March 2015)

[3] Privacy and Data Protection Act 2014, Part 1 – s 3

5. Relationship with Information Privacy Principle (IPP) 4 – Data security

Under IPP 4.1, your organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.[4] Your organisation should use the VPDSS as the primary reference point in complying with IPP4.1.

6. Purpose

The VPDSF has been developed to establish, monitor and assure security of information within the Victorian Government.

7. Objectives

The VPDSF has been developed to help Victorian public sector organisations:

- identify information and determine ownership
- assess the value of information
- identify and manage protective data security risks
- apply security measures
- create a positive security culture
- mature their protective data security capability.

8. Scope

The VPDSF provides your organisation with a minimum set of protective data security requirements across the four protective security domains. These requirements, coupled with assurance actions, are designed to assist you mitigate information security risks.

Where Victorian organisations handle information of national interest, the Protective Security Policy Framework (PSPF) requirements remain mandatory and supersede any obligations set out in the VPDSF.

The VPDSF should be read in conjunction with existing legislative obligations. Where relevant legislation mandates lower standards than those of the VPDSF, you are encouraged to meet the minimum requirements of the VPDSF.

[4] Privacy and Data Protection Act 2014, Schedule 1

9. Applicability

Section 84 of the PDP Act defines the organisations that are covered by the VPDSF as well as those that are exempt:

PDP Act Part Four, Section 84	
(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**.

The VPDSF applies equally to staff, contractors and consultants of public sector organisations identified in Section 84(1) of the PDP Act.

The VPDSF also extends to the protection of information collected or handled by any contracted service providers and external parties who are authorised by the Victorian Government to handle store, process or transmit information.

For more information on whether the VPDSF applies to your organisation, refer to the Resources section of our website.

9.1. Law Enforcement

9.1.1. Victoria Police

Victoria Police, as the primary Victorian law enforcement agency, obtain, receive, hold, and handle, sensitive information. This information is considered public sector data but, more importantly, is differentiated and given prominence under the PDP Act as *law enforcement data*.

Put simply, law enforcement data is information obtained, received, held, and handled by Victoria Police in the course of performing its law enforcement functions or activities.

Victoria Police has been bound by a set of protective data security standards since 2007. These standards, previously referred to as law enforcement data security standards, have evolved with various changes to the regulatory and legislative landscape. These changes include:

- the establishment of the Commissioner for Law Enforcement Data Security (CLEDS) (established under the *Commissioner for Law Enforcement Data Security Act 2005*)
- the evolution of CLEDS to the Commissioner for Privacy and Data Protection (CPDP) with the inclusion of privacy functions under the *Privacy and Data Protection Act 2014* (PDP Act)
- 2017 amendments to the PDP Act to merge the Offices of CPDP and the Freedom of Information Commissioner, and reflect the powers and functions of the inaugural Victorian Information Commissioner and their office, OVIC.

In October 2017, the Victorian Information Commissioner revoked the existing *Standards for Law Enforcement Data Security* (SLEDS) and bound Victoria Police to the VPDSF (including VPDSS and assurance model). Transition to the VPDSF brings Victoria Police in line with other public sector organisations to which the PDP Act applies.

Importantly, the VPDSF is consistent with the SLEDS, and will maintain the positive impact on Victoria Police's information management and security already achieved under the SLEDS.

9.1.2. Crime Statistics Agency

The Crime Statistics Agency (CSA) is responsible for processing, analysing and publishing Victorian Crime Statistics, independent of Victoria Police.[5]

The *Crime Statistics Act 2014* contains provisions that empower the Chief Statistician to receive law enforcement data from the Chief Commissioner of Victoria Police, and to publish and release crime statistics and research into crime trends.

Crime statistics data is delineated in the PDP Act as information (law enforcement data) received from Victoria Police under the relevant section within the *Crime Statistics Act 2014*, or information derived by the CSA from law enforcement data in the performance of functions under *Crime Statistics Act 2014*.

In November 2017, CSA transitioned from the *Crime Statistics Data Security Standards* (CSDSS) to the VPDSF (including VPDSS and assurance model).

[5] Crime Statistics Agency website. https://www.crimestatistics.vic.gov.au/about-us. Site accessed 10 January 2018.

10. Audience

This framework is intended for organisations (including employees, contractors and external parties) subject to the protective data security provisions of Part Four of PDP Act.

11. Compliance

Section 88 of the PDP Act outlines compliance requirements for applicable organisations:

PDP Act Part Four, Section 88	
(1)	A public sector body Head for an agency or a body to which this Part (Part Four) applies must ensure that the agency or body 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.
(2)	A public sector body Head for an agency or 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.

11.1. Implementation of the VPDSS by smaller organisations

If smaller organisations do not have sufficient staffing or budget to comply with all requirements of the standards, they may take a joint approach to implementation with a host organisation.

They may:

- use a host organisation’s systems, processes and existing information security policies and resources

or

- share information security resources and jointly develop information security policies and systems.

For information regarding reporting options for smaller organisations, refer to Part Five – Assurance Model.

12. Timeframes

Section 89 of the PDP Act outlines reporting and assurance activity timeframes:

PDP Act Part Four, Section 89	
(1)	Within 2 years after the issue of protective data security standards applying to an agency or body to which this Part applies, the public sector body Head must ensure that— (a) a security risk profile assessment is undertaken for the agency or body; and (b) 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.
(4)	A public sector body Head must ensure that the protective data security plan prepared under this section is reviewed— (a) if there is a significant change in the operating environment or the security risks relevant to the agency or body; or (b) otherwise, every 2 years.

13. Customised protective data security standards

In the unlikely event that an organisation requires a departure from the general VPDSS, it may seek customised protective data security standards under Section 86 of the PDP Act.

14. Review/audit

All controls within the VPDSF may be used as the basis for:

- internal and external annual audit programs
- any review or investigation by OVIC or the Victorian Auditor General's Office (VAGO)
- assurance purposes by other government organisations.

Part Two – The Framework

15. VPDSF structure

The VPDSF has:

- a tiered structure of interconnected security standards (VPDSS)
- supporting security guidance.

This provides a common model for implementation of the framework and obligations under the PDP Act. Implementation of the standards is monitored and measured using the Assurance Model, which overlays the framework.

High-level mandatory statements (standards and protocols) should be read in conjunction with their supporting controls. The diagram below shows the interlinked nature of each layer of the framework.

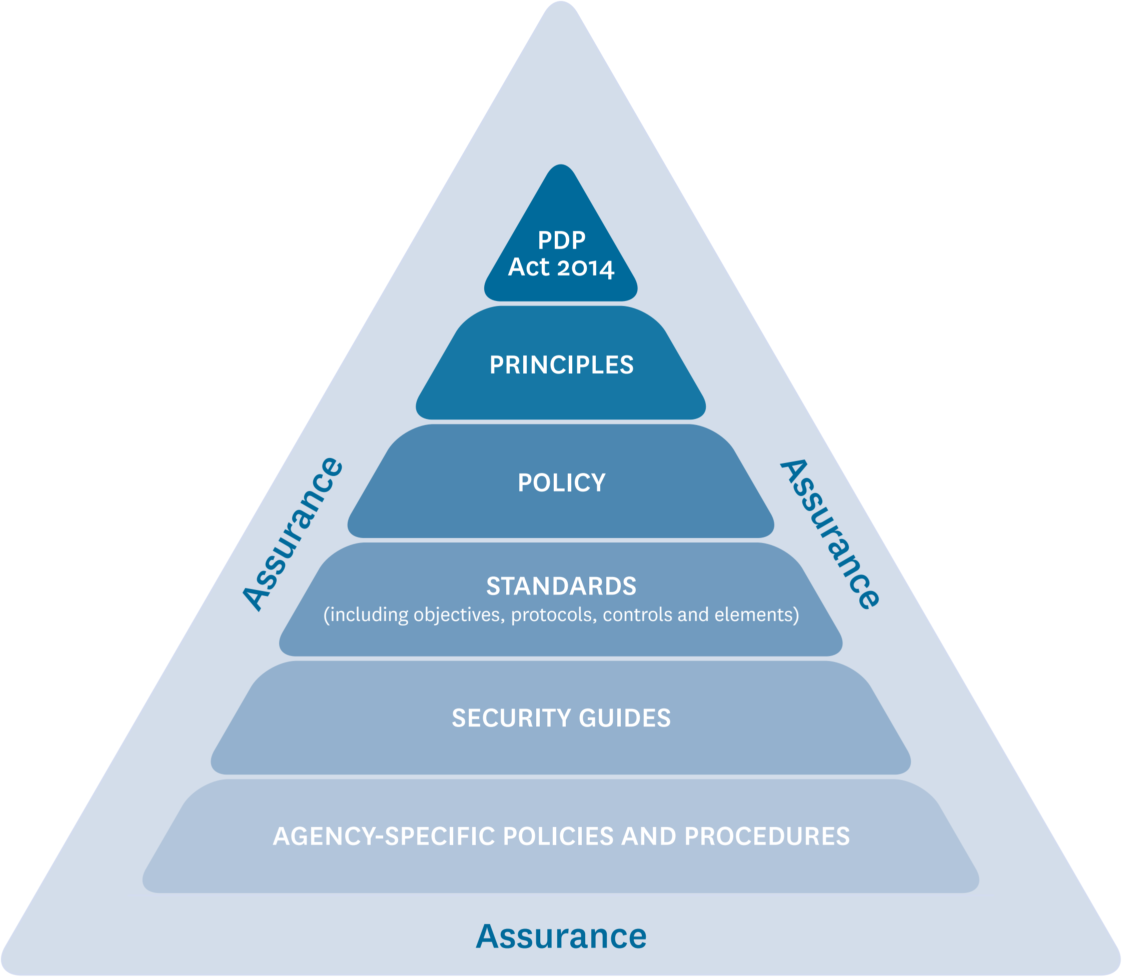

PDP
Act 2014
PRINCIPLES
POLICY
STANDARDS
(including objectives, protocols, controls and elements)
SECURITY GUIDES
AGENCY-SPECIFIC POLICIES AND PROCEDURES
Assurance
Assurance
Assurance

Figure 1. VPDSF structure

The following table explains the function of each layer.

VPDSF Tiers	Description	Outcomes
Privacy and Data Protection Act 2014	The Act provides for the responsible collection and handling of personal information in the Victorian public sector, and for the establishment of a protective data security framework for the Victorian public sector. The PDP Act empowers the Information Commissioner to develop, implement and oversee a comprehensive protective data security framework in Victoria, known as the Victorian Protective Data Security Framework (VPDSF).	Legislation
Guiding Principles	Underlying concepts that support the general themes of the VPDSF. Refer to Guiding Principles section.	Foundational concepts
Standard(s)	High-level statement describing what needs to be achieved.	**What** is required
Statement of objective	A statement of the intent identifying the desired outcome from compliance with a standard.	**Why** it's required
Protocol(s)	Four targeted statements specifying the minimum mandatory requirements that reflect a continuous improvement life cycle to improve the overall maturity of security implementation	The **end state** that organisations are to achieve
Control(s)	The baseline or minimum expected security measures representing better practice. References include Australian and International Standards, Federal government guidance and tailored security guides developed by OVIC.	**Baseline/ default** security measures
Element(s)	A security measure(s) extracted from the control references that provide high level guidance on the implementation of each standard.	
Security guide(s)	Non-mandatory instructions and advice designed to support the implementation of the standards.	**Key points** of consideration

VPDSF Tiers	Description	Outcomes
Organisational specific policies and procedures	Security policies and procedures of organisations, designed to reflect their unique operating requirements.	Governing direction
Assurance Model	Establishes monitoring and assurance obligations for both OVIC and the broader Victorian public sector.	**Reporting** security posture

16. Victorian Protective Data Security Standards

The Victorian Protective Data Security Standards (VPDSS) establish 18 high level mandatory requirements to protect public sector data and provide for governance across the four domains of information, personnel, ICT and physical security.

Each standard is supported by four protocols. This follows the continuous improvement process of plan, do, check, and act (see Guiding Principles for details). This enables your organisation to continually assess your security controls against any new or updated threats and vulnerabilities.

The standards:

- take into account the policy and operational responsibilities of the Victorian government
- respect the important role that Victorian public sector organisations play in delivering critical services
- reflect national and international approaches to security but are tailored to the Victorian government environment
- focus on the security of information, rather than all official assets
- identify information security and ICT security as individual yet equally important security domains
- require contracted service providers with direct or indirect access to information to adhere to the standards.

The standards are durable and take a risk management approach that empowers government business to function effectively, safely and securely.

17. Assurance Model

The Assurance Model enables your organisation to measure the maturity of your implementation of the VPDSS.

The model aims to:

- enhance the maturity of your organisation's protective data security practices
- provide assurance to government of the security of information.

Refer to Part Five – Assurance Model for more information.

18. Roles and responsibilities

The relationship between the office of OVIC and organisations identified under Part Four of the PDP Act is:

18.1. Office of the Victorian Information Commissioner

Part Six of the PDP Act details the functions and powers of OVIC for monitoring and assuring the security of public sector data. These include:

- establishing a regime and framework for monitoring and assuring public sector data security
- promoting responsible protective data security practices in the public sector
- monitoring and assurance activities, including audits, to ascertain compliance with data security standards
- formal reporting and recommendations regarding data security
- referring findings of monitoring and assurance activities, including audits, to an appropriate person or body for further action
- undertaking research relevant to protective data security in the Victorian public sector
- retaining copies of protective data security plans.

These functions enable OVIC to provide reasonable assurance to government that Victorian public sector organisations' protective data security risks are being managed effectively, and that their business goals and objectives will be achieved efficiently and economically.

18.2. Victorian public sector organisations

When applying the requirements of the VPDSF, your organisation must be aware of the legal or regulatory environment in which you operate.

All organisations identified in Part Four (s84) of the PDP Act have responsibilities regarding monitoring and assurance of their protective data security. These include:

- developing, implementing and maintaining a Security Risk Profile Assessment (SRPA)
- developing, implementing and maintaining a Protective Data Security Plan (PDSP)
- providing OVIC free and full access to data or data systems, when requested[6]
- participating in any monitoring or assurance conducted by OVIC, including providing information or documents when requested
- not engaging in a practice that contravenes a protective data security standard regarding public sector data collected, held, managed, used, disclosed or transferred; and public sector data systems
- ensuring that a contracted service provider of the organisation does not do an act or engage in a practice that contravenes a protective data security standard regarding public sector data collected, held, used, managed, disclosed or transferred by the provider for the organisation
- providing an attestation to OVIC
- performing and maintaining internal audit, assurance, risk management, business planning and investment activities, including risk management and assurance activities associated with all external entities.

[6] Privacy and Data Protection Act 2014, Part 6 – Division 2, s 106

18.3. RACI table

The following RACI (Responsible, Accountable, Consulted, Informed) table, is representative of sample activities of OVIC and Victorian public sector organisations.

Activity	Responsible	Accountable	Consulted	Informed
Develop and issue the VPDSF	OVIC	OVIC	Organisation	Organisation
Interpret the intent of the VPDSS	OVIC	OVIC	Organisation	Organisation
Establish the business context	Organisation	Organisation	Organisation	OVIC
Value information	Organisation	Organisation	OVIC	OVIC
Apply the VPDSS	Organisation	Organisation	OVIC	OVIC
Select, certify and accredit security measures within the specified control framework of the VPDSF	Organisation	Organisation	Organisation	OVIC
Security incident response and management	Organisation	Organisation	Organisation	OVIC
Conduct internal monitoring and report on the implementation of VPDSS	Organisation	Organisation	OVIC	OVIC

Activity	Responsible	Accountable	Consulted	Informed
Update security work programs to reflect agile/ changing business operations	Organisation	Organisation	OVIC	OVIC
Provide assurance through an attestation	Organisation	Organisation	Organisation	OVIC
Conduct external monitoring activities for the implementation of the VPDSF	OVIC	OVIC	Organisation	Organisation
Advise the Victorian Government of trends and themes identified by **OVIC**	OVIC	OVIC	Organisation	Organisation

19. Relationship with Whole of Victorian Government (WoVG)

The following entities play a key role in delivering effective, efficient and economic protective data security within the Victorian public sector.

Victorian Auditors General's Office (VAGO)

An independent officer of the Victorian Parliament, appointed to examine the management of resources within the public sector on behalf of Parliament and Victorians. VAGO may conduct independent performance audits of any protective data security area. These audits would be independent of any assurance activities of OVIC.

Public Record Office Victoria (PROV)

Responsible for standards and guidance relating to recordkeeping within Victoria, including compliance to the Public Records Act 1973. PROV issues standards regulating the creation, maintenance and security of public records including the retention and disposal of public records.

Department of Treasury and Finance (DTF)

Issuer of the Victorian Government Financial Management Control Framework, which includes obligations regarding security of financial systems and data; also issuer of the Victorian Government Risk Management Framework (VGRMF) which supports risk management within the Victorian public sector.

Victorian Managed Insurance Authority (VMIA)

Issuer of the risk management practice guide to support implementation of the VGRMF; also provider of risk services, including advice and training, to government.

Department of Premier and Cabinet (DPC) – Enterprise Solutions Branch (ESB)

Issuer of the Victorian Government Information Technology Strategy, Cyber Security Strategy and Information Management Framework.

Parliamentary Committees

Facilitate greater public input into issues considered by Parliament. This includes holding inquiries into issues which may include protective data security, and calling for wider community input from experts, individuals, business and government organisations.

This page is intentionally left blank.

Part Three – Guiding Principles

20. Overview

Given the vast volume of information processed or held by Victorian public sector organisations, secure management of information, assets and services is critical to Government service delivery, public safety and our way of life. By implementing protective security measures, our organisations can guard information against a range of threats.

These guiding principles of the framework enable your organisation to evaluate its current and prospective security practices:

1. Strong governance arrangements ensure the protective data security requirements of the business are reflected in organisational planning.
2. Risk management empowers an organisation to make informed decisions and prioritise security efforts.
3. Understanding information value informs an organisation's application of security measures to protect information.
4. A positive security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation allows an organisation to function effectively and support the delivery of government services.
5. A continuous improvement lifecycle model enables an organisation to systematically identify opportunities to mature its protective data security practices.
6. Sound protective data security practices assist an organisation to achieve its objectives in an efficient, effective and economic manner.

21. Governance

Principle 1: Strong governance arrangements ensure the protective data security requirements of the business are reflected in organisational planning.

The Australian National Audit Office (ANAO) defines 'public sector governance' as

> *How an organisation is managed, its corporate and other structures, its culture, its policies and strategies and the way it deals with its various stakeholders. The concept encompasses the manner in which public sector organisations acquit their responsibilities of stewardship by being open, accountable and prudent in decision- making, in providing policy advice, and in managing and delivering programs.* [7]

Given the wide variety and nature of organisations operating across the Victorian public sector, OVIC recognises that governance arrangements can take many forms. Under the VPDSF, your organisation is expected to establish security governance arrangements that reflect your individual circumstances, and base policies and processes on sound risk management. This approach balances the benefits and potential costs of protective data security activities, ensuring security measures reflect the value of information.

The evolving environment in which organisations operate, and the need for enhanced secure information-sharing practices across governments, point to the critical function that public sector governance plays.

[7] Australian National Audit Office Better Practice Guide, *Public Sector Governance*, Vol. 1 & 2, July 2003

By initiating robust governance arrangements, your organisation can direct and control processes for protection of your information. This includes public sector body Heads providing sponsorship in protective data security through authority, accountability, stewardship, leadership, direction and ensuring all personnel understand their role in information protection.

By embedding good governance policies and practices and ensuring these measures reflect changing needs, your organisation will better prepared to face the challenges of protective data security.

22. Risk management

Principle 2: Risk management empowers organisations to make informed decisions and prioritise security efforts.

Within Victorian Government risk management is defined as

> *the combination of organisational systems, processes and culture which facilitate the identification, assessment, evaluation and treatment of risk to achieve an appropriate balance between realising opportunities while minimising losses in the pursuit of strategic objectives*[8].

A risk management approach requires your organisation to ensure information is always adequately protected, by continually assessing security measures against any new or updated threats and vulnerabilities.

The adoption of a risk-based approach consistent with the Victorian Government Risk Management Framework (VGRMF) is the fundamental principle of the VPDSF. A flexible approach to implementation of security measures provides your organisation with the autonomy to interpret your business needs and articulate your risk tolerance within your operating environment.

Public sector body Heads are expected to understand, prioritise and manage security risks to prevent harm to information and disruption to business objectives.

23. Information value

Principle 3: Understanding information value informs an organisation's application of security measures to protect public sector data.

Value refers to the overall importance of information, based on a holistic assessment of compromise to the confidentiality, integrity and/or availability of information.

The overall value of information informs security measures needed to fully protect it. The VPDSF provides organisations with tools to assess this overall value.

[8] Department of Treasury and Finance, *Victorian Government Risk Management Framework* (VGRMF), (March 2015)

Confidentiality, Integrity and Availability (CIA) are widely recognised as the traditional security attributes of information management and are commonly referred to as the CIA triad.

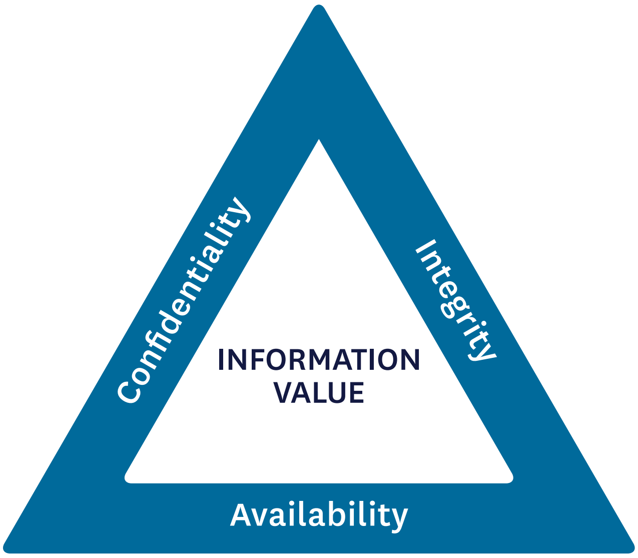


Figure 2. CIA Triad

Confidentiality	The limiting of official information to authorised persons for approved purposes (need to know).
Integrity	The assurance that information has been created, amended or deleted only by the intended, authorised means and is correct and valid.
Availability	The desired state that allows authorised persons to access particular information for authorised purposes, at the time they need to do so.

The VPDSF considers these three security attributes in an equal manner.

24. Security culture

Principle 4: A positive security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation allows an organisation to function effectively and support the delivery of government services.

Organisational culture is underpinned by the attitudes and behaviours of personnel and, in particular, their shared values and beliefs that interact with the organisation's structures and control systems to produce behavioural norms[9]. Behavioural norms influence the day-to-day operation of an organisation and act as a powerful and often subliminal force that shapes its very nature.

The VPDSF seeks to establish security as a natural element of organisational culture. To achieve this,

[9] B. Uttal, 'The corporate culture vultures', *Fortune Magazine*, Vol. 108, No. 8, October 1983

organisations must introduce cultural change where protective data security practices are reflected in everyday business operations, and all personnel take a shared responsibility. By embedding security in organisational culture, it becomes something that 'is', rather than something an organisation 'has' or 'does'.

A natural outcome of this cultural transformation program will:

- see personnel thinking and acting in more security-conscious ways
- help reduce organisations' protective data security risks
- enable the secure delivery of government services.

25. Continuous improvement (Plan, Do, Check, Act)

Principle 5: A continuous improvement lifecycle model enables an organisation to systematically identify opportunities to mature their protective data security practices.

A key concept used throughout the VPDSF is a continuous improvement lifecycle model, which is an underlying theme of international standards such as:

- AS/NZS ISO 31000 Risk management – Principles and guidelines
- ISO 9001 Quality management
- ISO 19600:2014 Compliance management systems.

This quality-driven philosophy is designed to integrate protective data security into an organisation's entire business practices and ensure that security management (like risk management, information management, personnel management, ICT management and physical management) is not a 'set and forget' exercise.

The framework therefore requires organisations to:

- **Plan – Contextualise their business objectives**: understand the business and its core functions, and plan accordingly.
- **Do – Integrate security measures proportionate to business risks**: enhance business operations.
- **Check – Consistently monitor business operations**: undertake monitoring and assurance activities to ensure that implemented security measures support the business objectives while minimising business risks.
- **Act – Review, validate and update business objectives, risks and operations based on lessons learnt**: ensure security measures are updated to support an agile business response to a dynamic environment.

By adopting this model, your organisation will systematically identify opportunities to mature your protective data security practices and secure information through all stages of its lifecycle.

26. Business objectives

Principle 6: Sound protective data security practices enable an organisation to achieve its business objectives in an efficient, effective and economic manner.

To deliver value to the Victorian Government and broader community, the VPS must transform the way it understands, uses and consumes information. This concept extends beyond the strict protective data security domains, and reflects important principles and themes of information management.

The December 2015 report by the Victorian Auditor General: *Access to Public Sector Information* stated that previous efforts to establish a “foundation of comprehensive and sound information management (IM) practices have been neglected”, resulting in organisations not properly understanding nor managing the information they hold.

Organisations must have confidence in information they use when doing business, to enable maximum value (efficiency), ensure the delivery of quality outcomes (effectiveness) and minimise costs (economy). By employing the protective data security measures of the VPDSF, your organisation can ensure the core attributes of your information (confidentiality, integrity and availability) are maintained, and have confidence that your information can be relied on to make quality decisions.

The VPDSF enables your organisation to continually refine your security measures and respond to the changing needs of your internal business and the broader operational environment, including delivering value to the VPS.

This page is intentionally left blank.

Part Four – The Victorian Protective Data Security Standards

27. Purpose

The purpose of the VPDSS is to provide a set of criteria for the consistent application of risk-managed security practices across Victorian government information.

28. Objectives

The VPDSS is developed to help Victorian public sector organisations:

- manage information throughout its lifecycle (creation to disposal)
- manage information across all the security domains (information, personnel, ICT, physical)
- manage security risks to information (CIA)
- manage external parties with access to information
- share information with other organisations with confidence
- minimise security incidents.

29. Protective Data Security Domains

The 18 standards are presented across governance and the four security domains and feature core messages, including:

Security Governance	(12 standards) Executive sponsorship of and investment in security management, utilising a risk based approach
Information Security	(Three standards) Protection of information, regardless of media or format (hard and soft copy material), across the information lifecycle from when it is created to when it is disposed
Personnel Security	(One standard) Engagement and employment of eligible and suitable people to access information
ICT Security	(One standard) Secure communications and technology systems processing or storing information
Physical Security	(One standard) Secure physical environment (i.e. facilities, equipment and services) and the application of physical security measures to protect information

30. VPDSS Supporting Material

Supporting material designed to assist organisations in their application of the VPDSS can be found in the Resources section of our website.

1 Security Management Framework

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain a security management framework proportionate to their size, resources and risk posture.

Statement of Objective

To ensure security governance arrangements are clearly established, articulated, supported and promoted across the organisation and to enable the management of security risks to public sector data.

Protocol 1.1

There is executive sponsorship of the security management framework, and it is embedded in the organisation's governance arrangements.

Protocol 1.2

The security management framework is implemented in the organisation's governance arrangements.

Protocol 1.3

The security management framework is appropriately monitored and reviewed in the organisation's governance arrangements.

Protocol 1.4

The organisation's governance arrangements are improved and the security management framework is updated to respond to the evolving security risk environment.

Controls

An organisation should align its security management framework with *ISO/IEC 27001: 2013 Information Security Management*.

This material should be referenced when conducting assessments against these standards.

2 Security Risk Management

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must utilise a risk management framework to manage security risks.

Statement of Objective

To ensure public sector data is protected through the identification and effective management of security risks across the core security domains.

Protocol 2.1

There is executive sponsorship of security risk management, and it is incorporated in the organisation's risk management framework.

Protocol 2.2

Security risks are identified and recorded in the organisation's risk register.

Protocol 2.3

Security risks are appropriately monitored and reviewed in the organisation's risk register.

Protocol 2.4

Security risk management is improved and the organisation's risk management framework is updated to respond to the evolving security risk environment.

Controls

An organisation should align its security risk management practices with the *VPDSF Assurance Collection: Chapter 1 – Protective Data Security Risk Profile Assessment* and the *Victorian Government Risk Management Framework (VGRMF)*.

Further consideration should also be given to the *ISO 31000:2009 Risk Management: Principles and guidelines* and *HB 167:2006 Security risk management*.

This material should be referenced when conducting assessments against these standards.

3 Security Policies and Procedures

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain security policies and procedures proportionate to their size, resources and risk posture.

Statement of Objective

To set clear strategic direction for the protection of public sector data.

Protocol 3.1

There is executive sponsorship of security requirements in the organisation’s policies and procedures.

Protocol 3.2

Security requirements are implemented in the organisation’s policies and procedures.

Protocol 3.3

Security requirements are appropriately monitored and reviewed in the organisation’s policies and procedures.

Protocol 3.4

Security requirements are improved and the organisation’s policies and procedures are updated to respond to the evolving security risk environment.

Controls

An organisation should align its security policies and procedures with the better practice guide *Developing agency protective security policies, plans and procedures* of the Protective Security Policy Framework (PSPF).

This material should be referenced when conducting assessments against these standards.

4 Information Access

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain an access management regime for access to public sector data.

Statement of Objective

To ensure access to public sector data is authorised and controlled across the core security domains.

Protocol 4.1

There is executive sponsorship of security requirements, and they are incorporated in the organisation's access management regime.

Protocol 4.2

Security requirements are implemented in the organisation's access management regime.

Protocol 4.3

Security requirements are appropriately monitored and reviewed in the organisation's access management regime.

Protocol 4.4

Security requirements are improved and the organisation's access management regime is updated to respond to the evolving security risk environment.

Controls

An organisation should align its access management regime with *ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls [Access control]*.

Further consideration should also be given to relevant provisions within the *NIST Special publication 800-53, Security and Privacy controls for Federal Information Systems and Organisations*.

This material should be referenced when conducting assessments against these standards.

5 Security Obligations

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must define, document, communicate and regularly review the security obligations of all persons with access to public sector data.

Statement of Objective

To ensure all persons with access to public sector data understand their security obligations.

Protocol 5.1

There is executive sponsorship of the security obligations of all persons, and they are incorporated in the organisation's personnel management regime.

Protocol 5.2

Security obligations are embedded into the daily functions and activities of all persons and reflected in the organisation's personnel management regime.

Protocol 5.3

Security obligations of all persons are appropriately monitored and reviewed in the organisation's personnel management regime.

Protocol 5.4

Security obligations of all persons are improved and the organisation's personnel management regime is updated to respond to the evolving security risk environment.

Controls

An organisation should align its security obligations of all persons with the better practice guide *Protective Security Guidelines Agency Personnel Security Responsibilities* and *Australian Government Personnel Security Protocol* of the Protective Security Policy Framework (PSPF).

This material should be referenced when conducting assessments against these standards.

6 Security Training and Awareness

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must ensure all persons with access to public sector data undertake security training and awareness.

Statement of Objective

To create and maintain a strong security culture that ensures that all persons understand the importance of security across the core security domains and their obligations to protect public sector data.

Protocol 6.1

There is executive sponsorship of a security training and awareness program, and it is incorporated in the organisation's personnel management regime.

Protocol 6.2

The security training and awareness program is implemented in the organisation's personnel management regime.

Protocol 6.3

The security training and awareness program is appropriately monitored and reviewed in the organisation's personnel management regime.

Protocol 6.4

The security training and awareness program is improved and the organisation's personnel management regime is updated to respond to the evolving security risk environment.

Controls

An organisation should align its security training and awareness program with the better practice guide *Protective Security Guidelines Agency Personnel Security Responsibilities [Security awareness training]* of the Protective Security Policy Framework (PSPF).

Further consideration should also be given to relevant provisions within *ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls [During Employment] and NIST Special publication 800-53 [Awareness and Training], Security and Privacy controls for Federal Information Systems and Organisations*.

This material should be referenced when conducting assessments against these standards.

7 Security Incident Management

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain a security incident management regime proportionate to their size, resources and risk posture.

Statement of Objective

To ensure a consistent approach to the management of security incidents, allowing timely corrective action to be taken for the protection of public sector data.

Protocol 7.1

There is executive sponsorship of security incident management activities, and they are incorporated in the organisation's incident management regime.

Protocol 7.2

Security incident management activities are implemented in the organisation's incident management regime.

Protocol 7.3

Security incident management activities are appropriately monitored and reviewed in the organisation's incident management regime.

Protocol 7.4

Security incident management activities are improved and the organisation's incident management regime is updated to respond to the evolving security risk environment.

Controls

An organisation should align its security incident management regime with the better practice guide *Reporting incidents and conducting security investigations guidelines* of the Protective Security Policy Framework (PSPF).

This material should be referenced when conducting assessments against these standards.

8 Business Continuity Management

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain a business continuity management program that addresses the security of public sector data.

Statement of Objective

To enhance an organisation's capability to prevent, prepare, respond, manage and recover from any event that affects the confidentiality, integrity and availability of public sector data.

Protocol 8.1

There is executive sponsorship of security requirements, and they are incorporated in the organisation's business continuity management program.

Protocol 8.2

Security requirements are implemented in the organisation's business continuity management program.

Protocol 8.3

Security requirements are appropriately monitored and reviewed in the organisation's business continuity management program.

Protocol 8.4

Security requirements are improved and the organisation's business continuity management program is updated to respond to the evolving security risk environment.

Controls

An organisation should align its business continuity management program with the *AS/NZ 5050:2010 Business Continuity – managing disruption – related risk*.

Further consideration should also be given to the *ISO 22301:2012 Societal security – Business continuity management systems – requirements* and better practice guide *Business Continuity Management – Building resilience in public sector entities* of the Australian National Audit Office (ANAO).

This material should be referenced when conducting assessments against these standards.

9 Contracted Service Providers

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must ensure that contracted service providers with access to public sector data, do not do an act or engage in a practice that contravenes the Victorian Protective Data Security Standards (VPDSS).

Statement of Objective

To ensure the protection of public sector data across the core security domains, through the appropriate inclusion of the VPDSS in any contracted service provider arrangements.

Protocol 9.1

Prior to the engagement of contracted service providers, the VPDSS are considered in the planning, development and scoping of the security requirements in the organisation's contracted service provider arrangements.

Protocol 9.2

Security requirements are embedded in the organisation's contracted service provider arrangements.

Protocol 9.3

Security requirements are appropriately monitored and reviewed in the organisation's contracted service provider arrangements.

Protocol 9.4

Security requirements are improved and the organisation's contracted service provider arrangements are updated to respond to the evolving security risk environment.

Controls

An organisation should align its security requirements for contracted service provider arrangements with the security governance guideline *Security of outsourced services and functions* of the Protective Security Policy Framework (PSPF).

Further consideration should also be given to the better practice guide by the Australian National Audit Office (ANAO) – *Developing and Managing Contracts*.

This material should be referenced when conducting assessments against these standards.

10 Government Services

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation that receives a government service from another organisation must ensure that the service complies with the Victorian Protective Data Security Standards (VPDSS) in respect to public sector data that is collected, held, used, managed, disclosed or transferred.

Statement of Objective

To provide assurance that the organisation's public sector data is protected when they receive a government service from another organisation.

Protocol 10.1

Prior to the receipt of a government service, the VPDSS are considered in the planning, development and scoping of security requirements in the organisation's government service agreements or arrangements.

Protocol 10.2

Security requirements are embedded in the organisation's government service agreements or arrangements.

Protocol 10.3

Security requirements are appropriately monitored and reviewed in the organisation's government service agreements or arrangements.

Protocol 10.4

Security requirements are improved and the organisation's government service agreements or arrangements are updated to respond to the evolving security risk environment.

Controls

An organisation should align its security requirements in government service agreements or arrangements with the *Australian Government protective security governance guidelines – Security of outsourced services and functions* of the Protective Security Policy Framework (PSPF).

Further consideration should also be given to the better practice guide by the Australian National Audit Office (ANAO) – *Developing and Managing Contracts*.

This material should be referenced when conducting assessments against these standards.

11 Security Plans

GOVERNANCE

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain a protective data security plan to manage their security risks.

Statement of Objective

To ensure that an organisation treats identified risks through informed business decisions, while applying cost-effective security controls to protect public sector data.

Protocol 11.1

There is executive sponsorship of the organisation's Security Risk Profile Assessment (SRPA) and Protective Data Security Plan (PDSP), and these are incorporated in business planning processes.

Protocol 11.2

Security risks are identified, assessed and recorded in the organisation's SRPA and risk treatments reflected in the organisation's PDSP. A current copy of the organisation's PDSP is given to the Office of the Victorian Information Commissioner.

Protocol 11.3

The organisation's SRPA and PDSP are appropriately monitored and reviewed in the business planning processes.

Protocol 11.4

Security planning processes are improved and the organisation's SRPA and PDSP is updated every two years or sooner, as required, due to a significant change in the operating environment or the security risks relevant to the organisation.

Controls

An organisation should align its security risk management processes with the *VPDSF Assurance Collection: Chapter 1 – Protective Data Security Risk Profile Assessment, Chapter 3 – Protective Data Security Plan* and the *Victorian Government Risk Management Framework (VGRMF)*.

Further consideration should also be given to the *AS/NZ ISO 31000:2009 Risk Management: Principles and guidelines* and *HB 167:2006 Security risk management*.

This material should be referenced when conducting assessments against these standards.

12 Compliance

GOVERNANCE

Standard

An organisation must perform an annual assessment of their implementation of the Victorian Protective Data Security Standards (VPDSS) and report their level of compliance to the Office of the Victorian Information Commissioner.

Statement of Objective

To promote the organisation's security capability and ensure adequate tracking of it's compliance with the VPDSS.

Protocol 12.1

There is executive sponsorship of security compliance activities, and these are incorporated in the organisation's compliance program.

Protocol 12.2

An annual assessment of the organisation's security compliance activities is performed and an attestation by the public sector body Head is submitted to the Office of the Victorian Information Commissioner.

Protocol 12.3

Security compliance activities are appropriately monitored and reviewed in the organisation's compliance program.

Protocol 12.4

Security compliance activities are improved and the organisation's compliance program is updated to meet the evolving security risk environment.

Controls

An organisation should align its security compliance activities with the *VPDSF Assurance Collection: Chapter 2 – Measuring and reporting implementation of the VPDSS* and the *AS ISO 19600:2015 Compliance Management Systems – Guidelines*.

This material should be referenced when conducting assessments against these standards.

13 Information Value

INFORMATION SECURITY

Victorian Protective Data Security Standards

Standard

An organisation must conduct an information assessment considering the potential compromise to the confidentiality, integrity and availability of public sector data.

Statement of Objective

To ensure an organisation uses consistent valuation criteria to assess public sector data that informs the appropriate controls for the protection of this information, across the core security domains.

Protocol 13.1

There is executive sponsorship of the organisation's application of the Business Impact Level (BIL) table and these are incorporated in the organisation's information management framework.

Protocol 13.2

The organisation's application of the BIL table is used during an information assessment, to determine the value of public sector data and reflected in the organisation's information management framework.

Protocol 13.3

The organisation's application of the BIL table and the value of public sector data is appropriately monitored and reviewed, in accordance with the organisation's information management framework.

Protocol 13.4

The information assessment process is improved (including application of the BIL table) and the organisation's information management framework is updated to respond to the evolving security risk environment.

Controls

An organisation should value its public sector data in accordance with the *VPDSF Information Security Management Collection: Chapter 1 – Identifying and Managing Information Assets* and *Chapter 2 – Understanding Information Value*.

This material should be referenced when conducting assessments against these standards.

14 Information Management

INFORMATION SECURITY

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain information security controls in their information management framework.

Statement of Objective

To ensure the organisation's public sector data is protected across all stages of its lifecycle.

Protocol 14.1

There is executive sponsorship of information security controls, and these are incorporated in the organisation's information management framework.

Protocol 14.2

Information security controls are implemented in the organisation's information management framework.

Protocol 14.3

Information security controls are appropriately monitored and reviewed in the organisation's information management framework.

Protocol 14.4

Information security controls are improved and the organisation's information management framework is updated to respond to the evolving security risk environment.

Controls

An organisation should align its information security controls with the *VPDSF Information Security Management Collection: Chapter 3 – Protective Markings, WoVG Information Management Principles* and the *Public Record Office of Victoria (PROV) Standards and Policies*.

Further consideration should also be given to the *DataVic Access Policy* and the information controls contained in the *Information Security Management Protocol* of the Protective Security Policy Framework (PSPF).

This material should be referenced when conducting assessments against these standards.

15 Information Sharing

INFORMATION SECURITY

Victorian Protective Data Security Standards

Standard

An organisation must ensure that security controls are applied when sharing public sector data.

Statement of Objective

To prevent unauthorised access of the organisation's public sector data, through the application of secure information sharing practices.

Protocol 15.1

There is executive sponsorship of secure information sharing practices, and these are incorporated in the organisation's information management framework.

Protocol 15.2

Secure information sharing practices are implemented in the organisation's information management framework.

Protocol 15.3

Secure information sharing practices are appropriately monitored and reviewed in the organisation's information management framework.

Protocol 15.4

Secure information sharing practices are improved and the organisation's information management framework is updated to respond to the evolving security risk environment.

Controls

An organisation should align its information sharing practices with principles consistent with the *ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls [Information transfer]*.

This material should be referenced when conducting assessments against these standards.

16 Personnel Lifecycle

PERSONNEL SECURITY

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain personnel security controls in their personnel management regime.

Statement of Objective

To ensure a secure environment by actively managing all persons continued suitability and eligibility to access the organisation's public sector data.

Protocol 16.1

There is executive sponsorship of personnel security controls, and these are incorporated in the organisation's personnel management regime.

Protocol 16.2

Personnel security controls are implemented in the organisation's personnel management regime.

Protocol 16.3

Personnel security controls are appropriately monitored and reviewed in the organisation's personnel management regime.

Protocol 16.4

Personnel security controls are improved and the organisation's personnel management regime is updated to respond to the evolving security risk environment.

Controls

An organisation should align its personnel security controls with *AS4811:2006 Employment Screening*, *National Identity Proofing Guidelines*, the *Personnel security management protocol* and the *Protective Security Guidelines Agency Personnel Security Responsibilities* of the Protective Security Policy Framework (PSPF).

This material should be referenced when conducting assessments against these standards.

17 Information Communications Technology (ICT) Lifecycle

ICT SECURITY

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain Information Communications Technology (ICT) security controls in their ICT management regime.

Statement of Objective

To ensure the organisation's public sector data is protected through the use of ICT security controls.

Protocol 17.1

There is executive sponsorship of ICT security controls, and these are incorporated in the organisation's ICT management regime.

Protocol 17.2

ICT security controls are implemented in the organisation's ICT management regime.

Protocol 17.3

ICT security controls are appropriately monitored and reviewed in the organisation's ICT management regime.

Protocol 17.4

ICT security controls are improved and the organisation's ICT management regime is updated to respond to the evolving security risk environment.

Controls

An organisation should align its ICT security controls with the *Information Security Manual* (ISM) published by the Australian Signals Directorate (ASD).

This material should be referenced when conducting assessments against these standards.

18 Physical Lifecycle

PHYSICAL SECURITY

Victorian Protective Data Security Standards

Standard

An organisation must establish, implement and maintain physical security controls in their physical management regime.

Statement of Objective

To maintain a secure environment where the organisation’s public sector data is protected through physical security measures (facilities, equipment and services).

Protocol 18.1

There is executive sponsorship of physical security controls, and these are incorporated in the organisation’s physical management regime.

Protocol 18.2

Physical security controls are implemented in the organisation’s physical management regime.

Protocol 18.3

Physical security controls are appropriately monitored and reviewed in the organisation’s physical management regime.

Protocol 18.4

Physical security controls are improved and the organisation’s physical management regime is updated to respond to the evolving security risk environment.

Controls

An organisation should align its physical security controls with the *Physical security management protocol* of the Protective Security Policy Framework (PSPF).

This material should be referenced when conducting assessments against these standards.

This page is intentionally left blank.

Part Five – Assurance Model

31. Purpose

The Assurance Model ensures the security capability in the Victorian public sector is as reported by organisations. OVIC will in turn incorporate organisational security capability in its reporting to government.

32. Objectives

The model is developed to:

- foster confidence in the protective data security practices of Victorian Government
- measure effectiveness, efficiency and economic implementation of protective data security practices within the Victorian public sector
- support organisations' compliance with protective data security provisions of the PDP Act and VPDSS
- empower risk-based decisions and thinking within the Victorian public sector regarding protective data security practices and capability
- promote accountability, integrity and continuous improvement within the Victorian public sector regarding protective data security
- regulate the protective data security environment across the Victorian public sector.

33. Summary of your organisation's obligations

To meet your obligations set out in the PDP Act and VPDSS, your organisation must complete these activities:

- undertake a Security Risk Profile Assessment (SRPA), an assessment of the current risks to your organisation's information assets
- complete a VPDSS self-assessment (referencing the VPDSS elements)
- develop a detailed Protective Data Security Plan (PDSP), providing a plan of action to address protective data security risks and capability improvement
- submit a high level PDSP including attestation to OVIC by 31 August 2018 and every two years thereafter (or sooner if there is significant organisational change)
- review the PDSP at least every two years (or sooner if there is significant organisational change)
- cooperate during monitoring and assurance activities conducted by OVIC, such as audits or reviews.

34. What is the Assurance Model?

The Assurance Model sets out activities led by OVIC designed to monitor and measure the protective data security practices within the Victorian public sector. Activities will typically foster a partnership approach with OVIC and take the form of consultations, engagement and reviews to assure organisations are:

- meeting their obligations as stated in the PDP Act
- applying protective data security measures commensurate with information value and organisational security risk profile.

These activities help establish a better understanding of each organisation's protective data security practices, including adherence to the VPDSS. More broadly, they provide a level of assurance regarding the protection of information across the Victorian government.

The Assurance Model drives improvements to protective data security practices, using the Plan, Do, Check, Act ('PDCA') cycle.

35. Intended benefits

The model delivers these benefits:

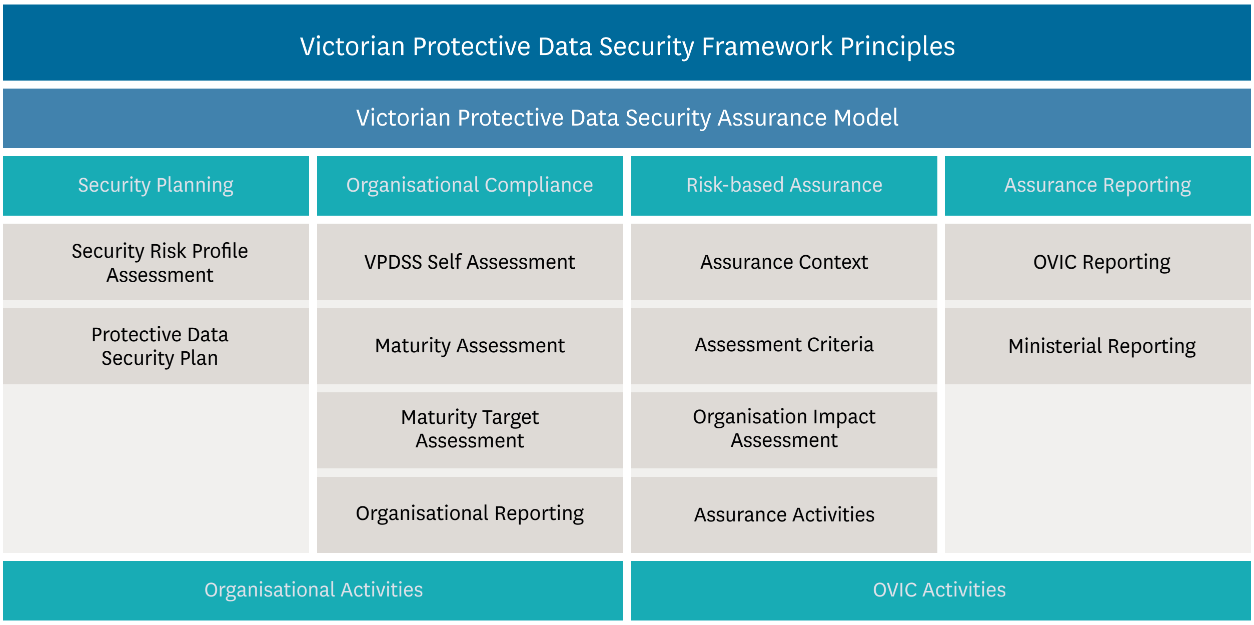
- provides organisations with a means of measuring their level of implementation of the protective data security provisions of the PDP Act and accompanying VPDSS
- enhances organisations' assessment of protective data security practices, risks and capability, resulting in informed decision making
- clearly establishes roles, responsibilities and accountabilities of all parties regarding protective data security practices within organisations
- identifies ways to assess protective data security risks and capability within organisations and across the Victorian public sector
- establishes tools to monitor the efficiency and effectiveness of protective data security practices across the Victorian public sector
- highlights the need for continuous improvement of protective data security practices across the Victorian public sector.

36. Assurance Model structure

The Assurance Model consists of these main areas:

- **Security planning** - activities used to assess organisational risk, capability and the development of an action plan.
- **Organisational Compliance** – a compliance approach based on a security capability maturity model which will support the continuous improvement principle of the VPDSS.
- **Risk-Based Assurance** – the assurance approach and supporting activities used by OVIC to assess the level, implementation and operating effectiveness of protective data security within the Victorian public sector. OVIC also uses this approach to plan, prioritise and determine the depth of assessment to be conducted.
- **Assurance reporting** - the reporting obligations and requirements for OVIC.

Each area is supported by operational components shown in the following diagram.



Victorian Protective Data Security Framework Principles

Victorian Protective Data Security Assurance Model

Security Planning	Organisational Compliance	Risk-based Assurance	Assurance Reporting
Security Risk Profile Assessment	VPDSS Self Assessment	Assurance Context	OVIC Reporting
Protective Data Security Plan	Maturity Assessment	Assessment Criteria	Ministerial Reporting
	Maturity Target Assessment	Organisation Impact Assessment	
	Organisational Reporting	Assurance Activities	

Organisational Activities

OVIC Activities

Figure 3. Assurance Model

36.1. Security planning

There are two core activities within the PDP Act that support a considered, planned and risk-based approach to protective data security:

Security Risk Profile Assessment (SRPA)	An assessment of the public sector organisation's protective data security risks
Protective Data Security Plan (PDSP)	A plan of action to address and improve protective data security of the organisation, including the mitigation of identified risks

The diagram below provides an overview of these requirements as well as the key components within each activity.

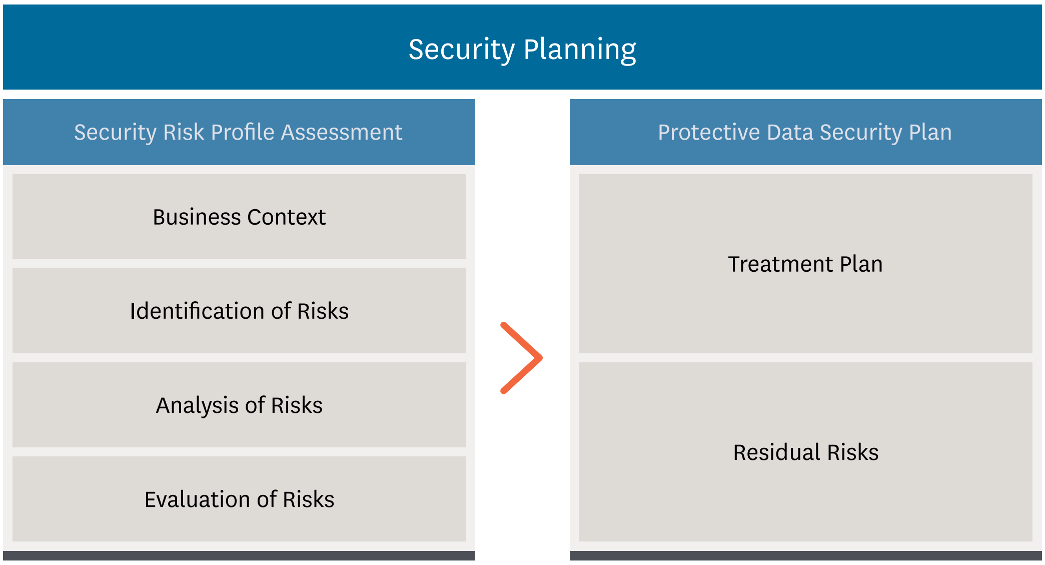


Figure 4. Security Planning requirements

The SRPA and PDSP are foundational components of a standard risk management process[9]. The SRPA is focused on an assessment of the organisation's protective data security risks, and directly informs the treatment plan within the PDSP.

The information contained in PDSPs will assist OVIC in its assurance activities.

To meet VPDSS 2 and 11, OVIC encourages organisations to undertake a SRPA and develop a PDSP drawing on the organisation's internal risk management practices (which should be consistent with the Victorian Government Risk Management Framework) and business planning processes, particularly:

- business goals and objectives
- business knowledge and risk strategies
- business opportunities and threat environment
- risk appetite
- risk management objectives and policy structures
- operational business processes
- organisational structure and extended enterprise
- consultation with business areas and related external parties.

Business planning and risk management are the responsibility of each public sector organisation, with consideration given to broader information management obligations including those associated with the *Financial Management Compliance Framework*, *Public Administration Act 2004*, *Health Records Act 2001*, *Public Records Act 1973* and Public Records Office Victoria Standards.

36.2. Organisational compliance

Organisations are required to assess their implementation of the VPDSS and report their level of compliance to OVIC.

[9] Department of Treasury and Finance, *Victorian Government Risk Management Framework* (VGRMF), (March 2015)

The Assurance Model adheres to the guiding principles of the framework by adopting a capability maturity model to support your organisation's internal self-assessment. The maturity ratings will enhance your organisation's visibility of current capabilities within protective data security practices and processes, and empower your organisation to identify opportunities to focus security uplift activities (target maturity ratings).

36.3. OVIC Risk-based assurance approach

OVIC has adopted a risk-based assurance approach to the scoping and prioritisation of assurance activities, including audits, reviews and monitoring activities. The model will take into account metrics such as:

- organisational control environment
- information value
- security risk profile to make informed decisions regarding the type, nature and priority of assurance activities.

36.4. Assurance reporting

Assurance reporting covers the reporting requirements and obligations of OVIC and the Minister, as specified in the PDP Act.

Internal reporting within a public sector organisation remains the responsibility of the organisation and is not covered by this framework.

36.4.1. Organisation's Assurance Reporting Timelines

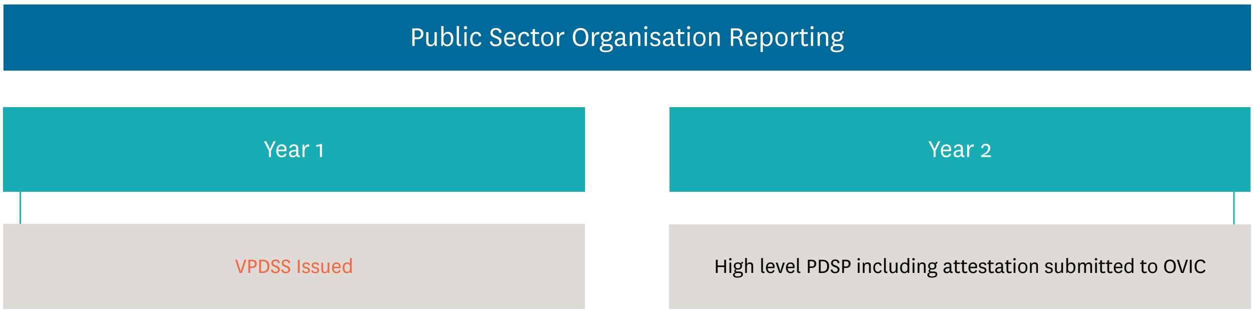

Public Sector Organisation Reporting
Year 1
Year 2
VPDSS Issued
High level PDSP including attestation submitted to OVIC

Figure 5. Public sector reporting

36.4.2. Organisations External Reporting Obligations

To support their protective data security reporting obligations, all Victorian public sector organisations covered by Part Four of the PDP Act are required to provide the deliverables in the following table to OVIC.

Deliverable	When	Required content
High level PDSP including attestation	1. Within 2 years after the issue of the VPDSS 2. Upon review resulting from any significant change to the operating environment or security risks 3. Upon internal biennial review (every 2 years)	Organisation's high level treatment plan including: Part A: Agency or Body details Part B: Compliance status and key activities (planned or in progress) Part C: Attestation

36.4.3. Single/Multiple organisation reporting

The following reporting options are designed to reflect the unique operating arrangements that exist across Victorian government.

This includes governance structures that often exist between larger lead agencies and smaller organisations that fall within the lead agency's portfolio of responsibilities and the provision of shared resources (including information technology and corporate functions). It also provides an opportunity for collaboration across agencies or bodies that perform a similar function.

Option 1 – An organisation submits a high level PDSP and provides an attestation on its own behalf only (**single organisation model**).

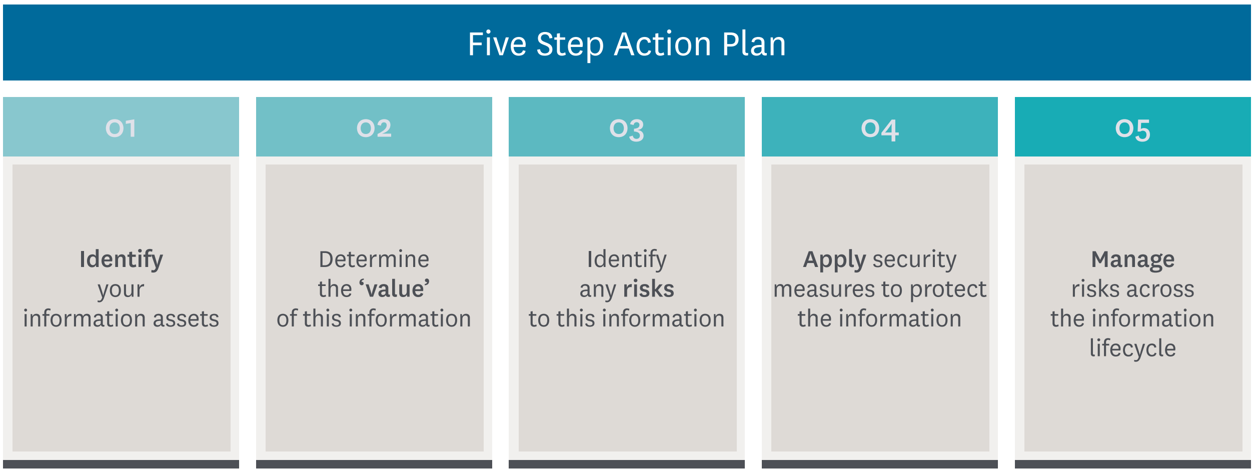
Option 2 – An organisation submits a consolidated high level PDSP and provides an attestation on its own behalf, and for and on behalf of one or more additional public sector agencies or bodies (**multiple organisation model**).

The multiple organisation model may be used in a portfolio setting where agencies or bodies fall within the portfolio of responsibilities of a Department or where a number of organisations of a similar form or function choose to consolidate their efforts.

OVIC does not mandate the use of any particular approach, with the selection of either reporting option residing with each organisation.

Part Six – VPDSF Five Step Action Plan

37. The Five Step Action Plan



Five Step Action Plan

01 **Identify** your information assets

02 Determine the **‘value’** of this information

03 Identify any **risks** to this information

04 **Apply** security measures to protect the information

05 **Manage** risks across the information lifecycle

Figure 6. VPDSF five step action plan

Figure six above shows the recommended five steps to inform the development of your Protective Data Security Plan and secure your organisation’s information assets. For some organisations, many of the activities will dovetail with existing security and information management practices that are already in place. For more information on the VPDSF Five step action plan refer to the Resources section of our website.

This page is intentionally left blank.

OVIC
Office of the Victorian
Information Commissioner

VICTORIA
State
Government