Office of the Victorian Information Commissioner

DATA PROTECTION

Victorian Protective Data Security Standards

March 2018

Freedom of Information | Privacy | Data Protection

Published by the Office of the Victorian Information Commissioner

PO Box 24274
Melbourne Victoria 3001

First Published July 2016

Amended March 2018

Also published on:
https://www.ovic.vic.gov.au

Contents

This page is intentionally left blank.

The Victorian Protective Data Security Standards

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.

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 agencies with confidence
- minimise security incidents.

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

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 Commissioner for Privacy and Data Protection.

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

Victorian Protective Data Security Standards

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 Commissioner for Privacy and Data Protection.

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 Commissioner for Privacy and Data Protection.

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.