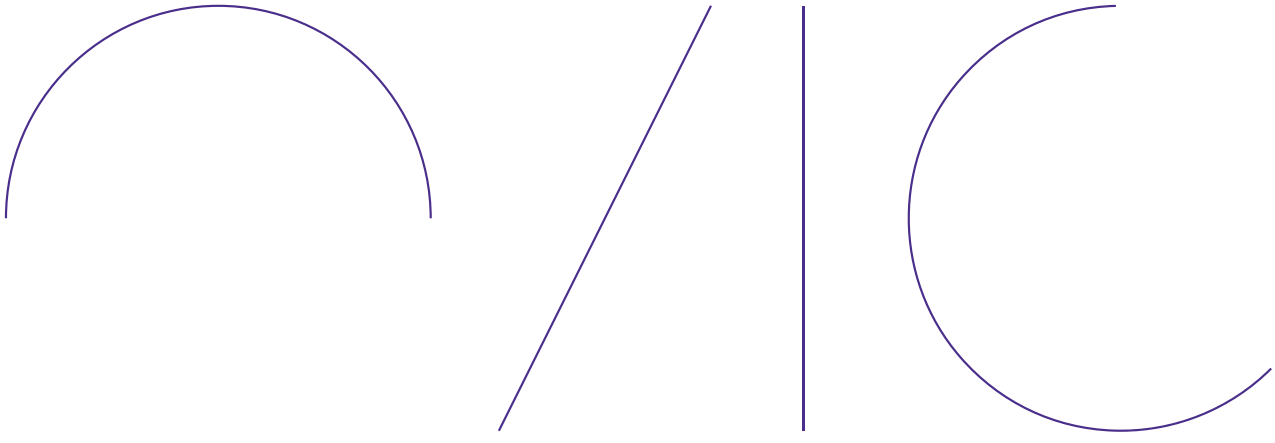
Office of the Victorian Information Commissioner

Victorian Protective Data Security Standards

Version 2.0

Implementation Guidance Version 2.4



Document details

Document details	Victorian Protective Data Security Standards
Publication date	January 2026
Review date	January 2027
Protective Marking	OFFICIAL
CM ref / location	D24/758[v2]
Document status	Published
Authority	Office of the Victorian Information Commissioner (OVIC)
Author	Information Security

Version Control

Version	Date	Additions/changes
1.0	June 2016	N/A
1.1	March 2018	Updated some control references
2.0	October 2019	• Removed protocols. • Integrated elements including: o a mapping to their primary control source. o providing old and new numbering. • Updated primary sources where the elements have been derived from. • Globally replace 'protective data security' with 'information security'. • Globally replace 'public sector data' with 'public sector information'. • Merged the following standards: 1, 3 2, 11 5, 6 9, 10, 15 13, 14 • Changed ordering of standards by moving 'Information Security Value' standard to be Standard 2.

Version	Date	Additions/changes
		• Replace Standard 12 – Compliance with new standard on reporting. • Globally change language to active voice. • Remove 'must' statements.
2.1	January 2021	• Add new sentence to Primary Sources description regarding use of dated vs. undated versions of references. • Remove VPDSS Element V1.1 reference column. • Update examples in the following elements: E6.060 E7.030 E8.080 E11.090 • Update Primary Sources for the following elements: E1.050 E2.020, E2.030, E2.050, E2.060, E2.070, E2.080, E2.090 E3.010, E3.020, E3.030, E3.040, E3.050 E4.040 E6.010, E6.020, E6.030, E6.040, E6.050 E8.020, E8.030, E8.080 E9.010, E9.040 E10.010, E10.020, E10.050, E10.070 E11.030, E11.040, E11.090, E11.110, E11.120, E11.180 E12.010, E12.030, E12.040 • Update outdated Appendix A links.
2.2	September 2023	• New OVIC branded template • Update out of date Primary Sources • Add Primary Sources to the following elements: E4.060 E5.050, E5.070 E10.010, E10.020, E10.060 E11.050, E11.140, E11.160 • Remove Primary Sources from the following elements: E2.050 E3.050 E5.050, E5.070 E6.030, E6.060 E8.020 E10.010 E11.050, E11.200 E12.020, E12.030

Version	Date	Additions/changes
		• Adjust E9.020 and E9.030 to align wording with legislation. • Update outdated Appendix A links.
2.3	February 2024	• Update Primary Sources for E9.020 and E9.030
2.4	January 2026	• Minor grammar updates • Add the section titles of all the referenced primary sources • Update Primary Sources for the following elements: E1.030 E2.030, E2.090 E3.010, E3.020, E3.040, E3.050 E4.040, E4.060 E5.010, E5.020, E5.030, E5.040, E5.060, E5.070 E6.010, E6.030, E6.040, E6.050, E6.060 E7.010, E7.030 E8.020, E8.030, E8.060, E8.080, E8.090 E9.010 E10.010, E10.020, E10.030, E10.040, E10.050, E10.060, E10.070, E10.080 E11.010, E11.020, E11.040, E11.090, E11.120, E11.180 E12.010, E12.020, E12.030, E12.040, E12.050, E12.060

Note. The issue of version 2.4 of this document **does not** represent a change to the Victorian Protective Data Security Standards (**VPDSS**) V2.0. This document has been reviewed for currency and updated accordingly under the VPDSS product development cycle.

Disclaimer

The information in this document is general in nature and does not constitute legal advice.

Copyright

Table of Contents

The purpose of the Victorian Protective Data Security Standards (**VPDSS**) is to provide a set of criteria for the consistent application of risk-based practices to manage the security of Victorian government information and systems. The Standards are issued under Parts 4 and 5 of the *Privacy and Data Protection Act 2014* (Vic).

Objectives

The VPDSS is developed to enable Victorian public sector organisations:

- manage public sector information throughout its lifecycle (creation to disposal)
- manage public sector information across all the security areas (governance, information, personnel, Information Communications Technology (**ICT**), physical)
- manage security risks to the confidentiality, integrity, and availability (often referred to as **CIA**) of public sector information
- manage external parties with access to public sector information
- share public sector information with other organisations with confidence
- minimise information security incidents.

Structure of the VPDSS

VPDSS Structure	Description	Outcome
Title	Heading/name of the standard	Key topic area (informational)
Standard	High-level statement describing what needs to be achieved by the organisation. There are 12 Victorian Protective Data Standards (**VPDSS**).	What is required (mandatory)
Statement of Objective	A statement of the intent of the standard identifying the desired outcome when the standard has been achieved.	Why it is required (informational)

VPDSS Structure	Description	Outcome
Element	A security measure(s) extracted from the source reference point that provides high level guidance.	How to? (risk-based action)
Primary Source	Reference point where the element has been primarily derived from for further implementation advice. For references that: • have a date, only the version cited applies, and • do not have a date, the latest version of the referenced document applies. References include Australian and International Standards, Federal and State government guidance and tailored guides developed by OVIC. Australian Standards can be accessed through the Victorian Government Library Service (**VGLS**) for eligible Victorian public sector organisations.	Need more information? (informational)

A Word on Elements

Elements are security measures that modify risk. Elements often depend on a supportive control environment to be effective. A control environment can be a set of standards, processes and structures, authorities, funds, and resources that provide the basis for applying controls across the organisation. The control environment therefore contributes to modifying risk indirectly.

The elements described in the VPDSS include both controls that directly modify risk and supportive controls that are essential to the control environment. Deciding which elements apply (statement of applicability), depends upon the organisation's criteria for risk acceptance and risk treatment options. Determining applicable elements also depends on the way in which elements interact with one another to provide 'defence in depth'.[1] Where an organisation believes elements do not apply to them, supporting justification should accompany such decisions.

[1] Defence in depth is a multi-layered system in which security measures combine to make it difficult for an intruder or authorised personnel to gain unauthorised access. This approach works on the premise that where one measure fails, there is another independent method in place to continue to defend. For further information refer to the NIST glossary https://csrc.nist.gov/glossary/term/defense_in_depth

Organisations should implement specific controls (which may be the element itself or multiple controls that fall under the element) appropriate to their organisation considering:

- their internal and external context
- the security value of the information and
- associated risks.

Whilst the elements have been logically grouped under their related topic area, i.e., elements related to physical security are listed under the physical security standard, selection of elements to mitigate risks may not be isolated to the specific topic area.

OVIC has referenced the primary source documents used for each element to give further information regarding implementation.

Organisations can design their own controls as required or identify them from any source that has at least functional equiveillance to, or is better than, the element identified by OVIC. These are recorded in an internal control library.

Standard 1 – Information Security Management Framework

Standard

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

Statement of Objective

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

Elements

V2.0 #	Element	Primary Source
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.	*AS/NZS ISO/IEC 27001:2023 Information security management systems – Requirements* § 4 Context of the organization § 5.2 Policy § 6.2 Information security objectives and planning to achieve them
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.	*AS/NZS ISO/IEC 27001:2023* § 4.2 Understanding the needs and expectations of interested parties

V2.0 #	Element	Primary Source
E1.030	The organisation's information security management framework aligns with its risk management framework.	*AS/NZS ISO/IEC 27001:2023* § 6.1 Actions to address risks and opportunities *AS ISO/IEC 27005:2014 Guidance on managing information security risks* § 5 Information security risk management
E1.040	Executive management defines information security functions, roles, responsibilities, competencies, and authorities.	*AS/NZS ISO/IEC 27001:2023* § 5.3 Organizational roles, responsibilities and authorities
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.	*OVIC Information security leads information sheet*
E1.060	Executive management owns, endorses, and sponsors the organisation's ongoing information security program(s) including the implementation plan.	*AS/NZS ISO/IEC 27001:2023* § 5.1 Leadership and commitment
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.	*AS/NZS ISO/IEC 27001:2023* § 9.1 Monitoring, measurement, analysis and evaluation § 9.2 Internal audit
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).	*AS/NZS ISO/IEC 27001:2023* § 7.1 Resources § 7.2 Competence
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.	*AS/NZS ISO/IEC 27001:2023* § 7.3 Awareness § 7.4 Communication
E1.100	The organisation documents its internal control library that addresses its information security risks.	*AS/NZS ISO/IEC 27001:2023* § 6.1 Actions to address risks and opportunities

V2.0 #	Element	Primary Source
E1.110	The organisation monitors, reviews, validates, and updates the information security management framework.	*AS/NZS ISO/IEC 27001:2023* § 9.3 Management review § 10.1 Continual improvement

Standard 2 – Information Security Value

Standard

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

Statement of Objective

To ensure an organisation uses consistent identification and assessment criteria for public sector information across its lifecycle to maintain its confidentiality, integrity and availability.

Elements

V2.0 #	Element	Primary Source
E2.010	The organisation's Information Management Framework incorporates all security areas.	*Victorian Government Information Management Framework* § Enabler: Security and Privacy § Enabler: Lifecycle Management
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.	*OVIC Practitioner Guide: Identifying and Managing Information Assets V2.0* § 9 Conducting an information review § 10 Define the organisation's information assets § 11 Information Asset Register (IAR) § 12 Continually review, validate and update the IAR

V2.0 #	Element	Primary Source
E2.030	The organisation uses a contextualised VPDSF business impact level (BIL) table to assess the security value of public sector information.	*OVIC Practitioner Guide: Assessing the security value of public sector information V2.0* § 12 Contextualising the VPDSF BIL table for an organisation *VPDSF Business Impact Level Table V2.1*
E2.040	The organisation identifies and documents the security attributes (confidentiality, integrity, and availability business impact levels) of its information assets in its information asset register.	*OVIC Practitioner Guide: Assessing the security value of public sector information V2.0* § 6 What information needs to undergo a security value assessment? § 7 Who performs an information security value assessment?
E2.050	The organisation applies appropriate protective markings to information throughout its lifecycle.	*OVIC Practitioner Guide: Protective markings V2.0* § 7 What information requires a protective marking? § 9 Protective markings scheme (Victoria)
E2.060	The organisation manages the aggregated (combined) security value of public sector information.	*OVIC Practitioner Guide: Assessing the security value of public sector information V2.0* § 8.4 Consider the combined security value of the information
E2.070	The organisation continually reviews the security value of public sector information across the information lifecycle.	*OVIC Practitioner Guide: Assessing the security value of public sector information V2.0* § 14 Information lifecycle and security value assessments

V2.0 #	Element	Primary Source
E2.080	The organisation manages externally generated information in accordance with the originator's instructions.	*OVIC Practitioner Guide: Protective markings V2.0* § 19 Protectively marked information from another organisation § 20 Commonwealth information § 21 Other State or Territory information § 22 Foreign Government information § 23 Private industry body markings § 24 Unfamiliar markings § 25 Information protectively marked under a former scheme
E2.090	The organisation manages the secure disposal (archiving/ destruction) of public sector information in accordance with its security value.	*Protective Security Policy Framework (**PSPF**) Release 2025* § 11 Information disposal

Standard 3 – Information Security Risk Management

Standard

An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks.

Statement of Objective

To ensure an organisation manages information security risks through informed business decisions while applying controls to protect public sector information.

Elements

V2.0 #	Element	Primary Source
E3.010	The organisation conducts security risk assessments and determines treatment plans in accordance with its risk management framework covering all the processes to manage information security risks including: Risk identification; Risk analysis; Risk evaluation; and, Risk treatment.	*OVIC Practitioner Guide: Information Security Risk Management V2.0* § 10 SRPA phases *AS/NZS ISO/IEC 27005:2024 Guidance on managing information security risks* § 7 Information security risk assessment process § 8 Information security risk treatment process § 9 Operation
E3.020	The organisation records the results of information security risk assessments and treatment plans in its risk register.	*OVIC Practitioner Guide: Information Security Risk Management V2.0* § 10.1 Recording risks *VMIA Develop a foundation-level organisational framework* § A Risk Register

V2.0 #	Element	Primary Source
E3.030	The organisation considers information security risks in organisational planning.	*VMIA Embedding risk thinking and techniques* § Show that you've considered risk in your strategies and plans
E3.040	The organisation communicates and consults with internal and external stakeholders during the information security risk management process.	*OVIC Practitioner Guide: Information Security Risk Management V2.0* § 8 Consultation *AS/NZS ISO/IEC 27005:2024* § 10.3 Communication and consultation
E3.050	The organisation governs, monitors, reviews, and reports on information security risk (e.g., operational, tactical and strategic through a risk committee (or equivalent, e.g., audit, finance, board, corporate governance)).	*OVIC Practitioner Guide: Information Security Risk Management V2.0* § 11 Ongoing maintenance *Victorian Government Risk Management Framework (**VGRMF**) September 2025* § 2.1.2 Agency audit committee *AS/NZS ISO/IEC 27005:2024* § 10.5 Monitoring and review *AS ISO 31000:2018 Risk management – Guidelines* § 6.7 Recording and reporting

Standard 4 – Information Access

Standard

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

Statement of Objective

To formally authorise and manage the physical and logical access to public sector information.

Elements

V2.0 #	Element	Primary Source
E4.010	The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know[2].	*AS/NZS ISO/IEC 27002:2022 Information security controls* § 5.15 Access control *SOD IDAM 01 – Workforce Identity and Access Management*[3] § IDAM Governance
E4.020	The organisation documents a process for managing identities and issuing secure credentials (registration and de-registration) for physical and logical access to public sector information.	*AS/NZS ISO/IEC 27002:2022* § 5.16 Identity management *SOD IDAM 01 – Workforce Identity and Access Management* § Enrolment
E4.030	The organisation implements physical access controls (e.g., key management, swipe card access, visitor passes) based on the principles of least-privilege and need-to-know.	*AS/NZS ISO/IEC 27002:2022* § 7.1 Physical security perimeters § 7.2 Physical entry

[2] The principles of restricting an individual's access to only the information they require to fulfil the duties of their role.

[3] The Victorian Government Workforce IDAM Statement of Direction (SOD) defines the whole of government vision for identity and access management. Whilst a government wide approach, the areas covered in this document can also be applied at a local organisation level.

V2.0 #	Element	Primary Source
E4.040	The organisation implements logical access controls (e.g., network account, password, two-factor authentication) based on the principles of least-privilege and need-to-know.	*AS/NZS ISO/IEC 27002:2022* § 5.17 Authentication information § 8.5 Secure authentication *Australian Government Information Security Manual (**ISM**) December 2025* § Guidelines for Personnel Security – Access to systems and their resources *Australian Signals Directorate (**ASD**) Essential Eight* § Restrict administrative privileges § Multi-factor authentication
E4.050	The organisation manages the end-to-end lifecycle of access by following provisioning and de-provisioning processes.	*AS/NZS ISO/IEC 27002:2022* § 5.18 Access rights *SOD IDAM 01 – Workforce Identity and Access Management* § Lifecycle Management
E4.060	The organisation limits the use of, and actively manages, privileged physical and logical access and separates these from normal access (e.g., executive office access, server room access, administrator access).	*AS/NZS ISO/IEC 27002:2022* § 8.2 Privileged access rights *SOD IDAM 01 – Workforce Identity and Access Management* § Privileged Access *ASD Essential Eight* § Restrict administrative privileges
E4.070	The organisation regularly reviews and adjusts physical and logical access rights taking into account operational changes.	*AS/NZS ISO/IEC 27002:2022* § 5.18 Access rights

Standard 5 – Information Security Obligations

Standard

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

Statement of Objective

To create and maintain a strong security culture by ensuring that all persons understand the importance of information security across all the security areas and their obligations for protecting public sector information.

Elements

V2.0 #	Element	Primary Source
E5.010	The organisation documents its information security obligations and communicates these to all persons with access to public sector information (e.g., policies, position descriptions).	*Protective Security Policy Framework (**PSPF**) Release 2025* § 3.2 Security practices and procedures § 3.4 Positive security culture *AS/NZS ISO/IEC 27002:2022 Information security controls* § 5.2 Information security roles and responsibilities § 5.4 Management responsibilities § 6.2 Terms and conditions of employment
E5.020	The organisation's information security training and awareness content covers all security areas.	*PSPF Release 2025* § 3.5 Security awareness training *PSPF Guidelines 2025* § 3.5.4 Content of security awareness training

E5.030	The organisation delivers information security training and awareness to all persons with access to public sector information, upon engagement and at regular intervals thereafter in accordance with its training and awareness program and schedule.	*PSPF Release 2025* § 3.5 Security awareness training *AS/NZS ISO/IEC 27002:2022* § 6.3 Information security awareness, education and training
E5.040	The organisation provides targeted information security training and awareness to persons in high-risk functions or who have specific security obligations (e.g., executives, executive assistants, procurement advisors, security practitioners, risk managers).	*PSPF Release 2025* § 3.5 Security awareness training *PSPF Guidelines 2025* § 3.5.5 Additional content for security-cleared personnel § 3.5.6 Additional content for high-risk positions
E5.050	The organisation reviews and updates the information security obligations of all persons with access to public sector information.	*AS/NZS ISO/IEC 27002:2022* § 6.2 Terms and conditions of employment
E5.060	All persons with access to public sector information acknowledge their information security obligations at least annually (e.g., during performance development discussions, attending security briefings, completing security training).	*PSPF Guidelines 2025* § 21.3.1.2 Performance management[4]
E5.070	The organisation monitors, reviews, validates, and updates its information security training and awareness program and schedule.	*PSPF Guidelines 2025* §3.5.7 Security awareness refresher training

[4] Whilst this section originates from the overarching security clearance section of the PSPF, the techniques and approaches covered in this section can also be applied to non-clearance subjects based on the risk profile.

Standard 6 – Information Security Incident Management

Standard

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

Statement of Objective

To ensure a consistent approach for managing information security incidents, in order to minimise harm/damage to government operations, organisations or individuals.

Elements

V2.0 #	Element	Primary Source
E6.010	The organisation documents and communicates processes and plan(s) for information security incident management covering all security areas.	*OVIC Guide to developing an Information Security Incident Management Framework (**ISIMF**) V2.0* § A Plan and prepare *AS/NZS ISO/IEC 27002:2022 Information security controls* § 5.24 Information security incident management planning and preparation *Protective Security Policy Framework (**PSPF**) Release 2025* § 3.6 Security incidents *Victorian Government cyber incident response plan template*
E6.020	The organisation articulates roles and responsibilities for information security incident management.	*ISIMF* § A Plan and prepare *AS/NZS ISO/IEC 27002:2022* § 5.24 Information security incident management planning and preparation

V2.0 #	Element	Primary Source
E6.030	The organisation's information security incident management processes and plan(s) contain the five phases of: Plan and prepare; Detect and report; Assess and decide; Respond (contain, eradicate, recover, notify); and, Lessons learnt.	*AS/NZS ISO/IEC 27035.1:2025 Information security incident management Part 1: Principles and process* § 5 Process *ISIMF* § A Plan and prepare *Victorian Government Cyber Security Incident Management Plan* § Defining and categorising cyber security incidents
E6.040	The organisation records information security incidents in a register.	*AS/NZS ISO/IEC 27035.2:2025 Information security incident management Part 2: Guidelines to plan and prepare for incident response* § Annex B.2.2 Example items of the record for information security incident
E6.050	The organisation's information security incident management procedures identify and categorise administrative (e.g., policy violation) incidents in contrast to criminal incidents (e.g., exfiltrating information to criminal associations) and investigative handover.	*ISIMF* § D Respond *AS/NZS ISO/IEC 27035.1:2025* § 5.2 Plan and prepare § Annex D Considerations of situations discovered during the investigation of an incident
E6.060	The organisation regularly tests (e.g., annually) its incident response plan(s).	*AS/NZS ISO/IEC 27035.2:2025* § 11 Testing the information security incident management plan

Standard 7 – Information Security Aspects of Business Continuity and Disaster Recovery

Standard

An organisation embeds information security continuity in its business continuity and disaster recovery processes and plans.

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 information.

Elements

V2.0 #	Element	Primary Source
E7.010	The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas.	*AS/NZS ISO/IEC 27002:2022 Information security controls* § 5.29 Information security during disruption § 5.30 ICT readiness for business continuity
E7.020	The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans.	*AS/NZS ISO/IEC 27002:2022* § 5.29 Information security during disruption
E7.030	The organisation regularly tests (e.g., annually) its business continuity and disaster recovery plan(s).	*AS/NZS ISO/IEC 27002:2022* § 5.29 Information security during disruption § 5.30 ICT readiness for business continuity

Standard 8 – Third Party Arrangements

Standard

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

Statement of Objective

To confirm that the organisation's public sector information is protected when the organisation interacts with a third party.

Elements

V2.0 #	Element	Primary Source
E8.010	The organisation's information security policies, procedures and controls cover the entire lifecycle of third-party arrangements (e.g., contracts, MOUs and information sharing agreements).	*AS/NZS ISO/IEC 27002:2022 Information security controls* § 5.19 Information security in supplier relationships
E8.020	The organisation includes requirements from all security areas in third party arrangements (e.g., contracts, MOUs and information sharing agreements) in accordance with the security value of the public sector information.	*Protective Security Policy Framework (**PSPF**) Release 2025* § 6.1 Procurement, outsourcing and contract management *PSPF Guidelines 2025* § 6.1.1.1 Protective security terms and conditions *AS/NZS ISO/IEC 27002:2022* § 5.20 Addressing information security within supplier agreements § 6.6 Confidentiality or non-disclosure agreements

V2.0 #	Element	Primary Source
E8.030	The organisation undertakes an information security risk assessment of the third party's service offering and addresses any residual risks prior to finalising the arrangement.	*PSPF Release 2025* § 6 Third party risk management *PSPF Guidelines 2025* § 6.1.1 Procurement of outsourced services - Table 15: Examples of potential procurement security risks
E8.040	The organisation identifies and assigns information security roles and responsibilities in third party arrangements (e.g., contracts, MOUs and information sharing agreements).	*AS/NZS ISO/IEC 27002:2022* § 5.14 Information transfer
E8.050	The organisation establishes, maintains, and reviews a register of third-party arrangements (e.g., contracts, MOUs and information sharing agreements).	*AS/NZS ISO/IEC 27002:2022* § 5.20 Addressing information security within supplier agreements
E8.060	The organisation monitors, reviews, validates, and updates the information security requirements of third-party arrangements and activities.	*PSPF Release 2025* § 6.1.2 Ongoing management of security in contracts *AS/NZS ISO/IEC 27002:2022* § 5.21 Managing information security in the ICT supply chain § 5.22 Monitoring, review and change management of supplier services *Privacy and Data Protection Act 2014 (Vic) (**PDP Act**)* § 89 (3) Protective data security plans
E8.070	The organisation documents its information release management requirements (e.g., social media, news, DataVic).	*IM-GUIDE-06 Victorian Government Information Management Governance Guidelines* § Custodianship model *DataVic access policy guidelines*

V2.0 #	Element	Primary Source
E8.080	The organisation manages the delivery of maintenance activities and repairs (e.g., on-site, and off-site).	*AS/NZS ISO/IEC 27002:2022* § 7.13 Equipment maintenance *Australian Government Information Security Manual (**ISM**) December 2025* § Guidelines for information technology equipment – IT equipment maintenance and repairs
E8.090	The organisation applies appropriate security controls upon completion or termination of a third-party arrangement (e.g., contracts, MOUs and information sharing agreements).	*PSPF Release 2025* § 6.1.2 Ongoing management of security in contracts *PSPF Guidelines 2025* § 6.1.2.3 Complete or terminate contracts

Standard 9 – Information Security Reporting to OVIC

Standard

An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (**VPDSS**) and reports to the Office of the Victorian Information Commissioner (**OVIC**).

Statement of Objective

To promote the organisation's security capability and ensure adequate tracking of its exposure to information security risks.

Elements

V2.0 #	Element	Primary Source
E9.010	The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level (BIL) of 2 (limited) or higher.[5]	*OVIC Information Security Incident Notification Scheme V3.0*
E9.020	The organisation submits a copy of its Protective Data Security Plan (PDSP) to OVIC every two years.	*Privacy and Data Protection Act 2014 (Vic) (**PDP Act**)* § 89 Protective data security plans
E9.030	Upon significant change, the organisation submits a copy of its reviewed PDSP to OVIC.	*PDP Act* § 89 Protective data security plans
E9.040	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.	*Victorian Protective Data Security Framework (**VPDSF**) V2.1* § 9.3 Timeframes and deliverables in practice

[5] Refer to the current VPDSF BIL table on the OVIC website https://ovic.vic.gov.au/information-security/information-security-resources/ for further information.

Standard 10 – Personnel Security

Standard

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

Statement of Objective

To mitigate an organisation's personnel security risks and provide a consistent approach for managing all persons with access to public sector information.

Elements

V2.0 #	Element	Primary Source
E10.010	The organisation's personnel security policies and procedures address the personnel lifecycle phases of: Pre-engagement (eligibility and suitability); Engagement (ongoing and re-engagement); and, Separating (permanently or temporarily).	*Protective Security Policy Framework (**PSPF**) Guidelines 2025* § 16 Pre-employment eligibility § 17 Access to resources § 21 Maintenance and ongoing assessment § 22 Separation *AS 4811:2022 Workforce Screening* § 2.8.2 Basic requirements and guidance
E10.020	The organisation verifies the identity of personnel, re-validates, and manages any changes as required.	*PSPF Release 2025* § 16.1.1.1 Identity checks *National Identity Proofing Guidelines (**NIPG**) 2025* § Chapter 3 Verifying identity *AS 4811:2022* § 2.8.5.3 Identity

V2.0 #	Element	Primary Source
E10.030	The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.	*PSPF Release 2025* § 16.1 Pre-employment screening *AS 4811:2022* § 2.7 Risk management
E10.040	The organisation manages ongoing personnel eligibility and suitability requirements commensurate with its security and probity obligations and risk profile.	*PSPF Guidelines 2025* § 21.3 Sponsoring entities maintenance responsibilities[6] *AS 4811:2022* § 2.8.8 Screening lifecycle
E10.050	The organisation manages personnel separating from the organisation commensurate with its security and probity obligations and risk profile.	*PSPF Release 2025* § 22 Separation
E10.060	The organisation develops security clearance policies and procedures to support roles requiring high assurance and/ or handling security classified information.	*PSPF Release 2025* § 18 Security clearances *AS 4811:2022* § 2.7 Risk management
E10.070	The organisation undertakes additional personnel screening measures commensurate with the risk to support roles requiring high assurance and/ or handling security classified information.	*PSPF Release 2025* § 19.3 Minimum personnel security checks[7] *PSPF Guidelines 2025* § 19.3.17 Additional personnel security checks *AS 4811:2022* § 2.7 Risk management § 2.8.4.3 Eligibility and suitability

[6] Whilst this section originates from the overarching security clearance section of the PSPF, the techniques and approaches covered in this section can also be applied to non-clearance subjects based on the risk profile.

[7] Whilst this section originates from the overarching security clearance section of the PSPF, the techniques and approaches covered in this section can also be applied to non-clearance subjects based on the risk profile.

V2.0 #	Element	Primary Source
E10.080	The organisation actively monitors and manages security clearance holders.	*PSPF Guidelines 2025* § 19.5.1 Conditional security clearances § 21.1 Security clearance maintenance § 21.3 Sponsoring entities maintenance responsibilities § 22.3 Post-separation security clearance actions

Standard 11 – Information Communications Technology (ICT) Security

Standard

An organisation establishes, implements and maintains Information Communications Technology security controls.

Statement of Objective

To maintain a secure environment by protecting the organisation's public sector information through ICT security controls.

Elements

V2.0 #	Element	Primary Source
E11.010	The organisation manages security documentation for its ICT systems (e.g., system security plans).	*Australian Government Information Security Manual (**ISM**) December 2025* § Guidelines for cyber security documentation
E11.020	The organisation manages all ICT assets (e.g., on-site, and off-site) throughout their lifecycle.	*ISM* § Guidelines for physical security § Guidelines for information technology equipment
E11.030	The organisation conducts a security assessment for authorising systems to operate prior to transmitting, processing, or storing public sector information.	*ISM* § Applying a risk-based approach to cyber security – Authorise the system

V2.0 #	Element	Primary Source
E11.040	The organisation undertakes risk-prioritised vulnerability management activities (e.g., patch management, penetration testing, continuous monitoring systems).	*ISM* § Guidelines for system management – System patching § Guidelines for system monitoring - Event log monitoring *ASD Essential Eight* § Patch applications § Patch operating systems
E11.050	The organisation documents and manages changes to ICT systems.	*AS/NZS ISO/IEC 27002:2022 Information security controls* § 8.32 Change management
E11.060	The organisation manages communications security controls (e.g., cabling, telephony, radio, wireless networks).	*ISM* § Guidelines for communications infrastructure § Guidelines for communications systems § Guidelines for networking – Wireless networks § Guidelines for physical security – Facilities and systems - Bringing radio frequency and infrared devices into facilities
E11.070	The organisation verifies the vendors security claims before implementing security technologies.	*ISM* § Guidelines for evaluated products
E11.080	The organisation manages security measures (e.g., classification, labelling, usage, sanitisation, destruction, disposal) for media.	*ISM* § Guidelines for media

V2.0 #	Element	Primary Source
E11.090	The organisation manages standard operating environments (**SOEs**) for all ICT assets, including end user access devices (e.g., workstations, mobile phones, laptops), network infrastructure, servers, and Internet of Things (**IoT**) commensurate with security risk.	*ISM* § Guidelines for system hardening *ASD Essential Eight* § Application control § Configure Microsoft Office macros § User application hardening
E11.100	The organisation manages security measures for email systems.	*ISM* § Guidelines for email
E11.110	The organisation logs system events and actively monitors these to detect potential security issues (e.g., intrusion detection/ prevention systems (**IDS/ IPS**)).	*ISM* § Guidelines for system monitoring § Guidelines for networking - Network design and configuration - Using network-based intrusion detection and prevention systems
E11.120	The organisation uses secure system administration practices.	*ISM* § Guidelines for system management – System administration § Guidelines for personnel security - Access to systems and their resources *ASD Essential Eight* § Restrict administrative privileges
E11.130	The organisation designs and configures the ICT network in a secure manner (e.g., segmentation, segregation, traffic management, default accounts).	*ISM* § Guidelines for networking

V2.0 #	Element	Primary Source
E11.140	The organisation manages a process for cryptographic keys (e.g., disk encryption, certificates).	*ISM* Guidelines for cryptography - Cryptographic fundamentals - Cryptographic key management processes and procedures *AS/NZS ISO/IEC 27002:2022* § 8.24 Use of cryptography
E11.150	The organisation uses cryptographic controls for confidentiality, integrity, non-repudiation, and authentication commensurate with the risk to information.	*ISM* § Guidelines for cryptography
E11.160	The organisation manages malware prevention and detection software for ICT systems.	*ISM* § Guidelines for gateways § Guidelines for data transfers *AS/NZS ISO/IEC 27002:2022 controls* § 8.7 Protection against malware
E11.170	The organisation segregates emerging systems from production systems (e.g., physical and/ or logical) until their security controls are validated.	*ISM* § Guidelines for software development
E11.180	The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing, retention).	*ISM* § Guidelines for system management – Data backup and restoration *ASD Essential Eight* § Regular backups
E11.190	The organisation manages a secure development lifecycle covering all development activities (e.g., software, web-based applications, operational technology (Supervisory Control and Data Acquisition/ Industrial Control Systems (SCADA/ICS)).	*ISM* § Guidelines for software development

V2.0 #	Element	Primary Source
E11.200	The organisation manages security measures for enterprise mobility (e.g., mobile device management, working from home).	*ISM* § Guidelines for enterprise mobility *AS/NZS ISO/IEC 27002:2022* § 6.7 Remote working

Standard 12 – Physical Security

Standard

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

Statement of Objective

To maintain a secure environment by protecting the organisation's public sector information through physical security controls.

Elements

V2.0 #	Element	Primary Source
E12.010	The organisation plans and documents physical security measures.	*Protective Security Policy Framework (**PSPF**) Release 2025* § 23 Physical security lifecycle § 24 Security zones § 25 Physical security measures and controls
E12.020	The organisation applies defence-in-depth physical security measures.	*PSPF Release 2025* § 23 Physical security lifecycle § 24 Security zones § 25 Physical security measures and controls *AS/NZS ISO/IEC 27002:2022 Information security controls* § 7 Physical controls

V2.0 #	Element	Primary Source
E12.030	The organisation selects physical security measures commensurate with the business impact level of the information.	*PSPF Release 2025* § 23 Physical security lifecycle § 25 Physical security measures and controls *AS/NZS ISO/IEC 27002:2022* § 7 Physical controls
E12.040	The organisation has scalable physical security measures ready for activation during increased threat situations.	*PSPF Release 2025* § 23 Physical security lifecycle § 24 Security zones § 25 Physical security measures and controls *PSPF Guidelines 2025* § 3.1.3.10 Element: Threat levels § 3.1.4 Security plan review § 24.2.3 Security zone recertification and reaccreditation
E12.050	The organisation implements physical security measures when handling information out of the office.	*PSPF Guidelines 2025* § 7.1.4 International travel § 9.3 Minimum protections and handling requirements § 17.3 Remote access to resources *AS/NZS ISO/IEC 27002:2022* § 7.9 Security of assets off-premises
E12.060	The organisation manages physical security measures throughout their lifecycle.	*PSPF Release 2025* § 23 Physical security lifecycle § 24 Security zones § 25 Physical security measures and controls *AS/NZS ISO/IEC 27002:2022* § 7 Physical controls

Appendix A - VPDSS Primary Sources

Victorian Government

Privacy and Data Protection Act 2014 (Vic) (**PDP Act**)

https://www.legislation.vic.gov.au/in-force/acts/privacy-and-data-protection-act-2014/

Office of the Victorian Information Commissioner:

https://ovic.vic.gov.au/information-security/information-security-resources/

Victorian Protective Data Security Framework (**VPDSF**) V2.1

Information Sheet: Information Security Leads

Practitioner Guide: Identifying and Managing Information Assets V2.0

Practitioner Guide: Assessing the security value of public sector information V2.0

Business Impact Level Table V2.1

Practitioner Guide: Protective Markings V2.0

Practitioner Guide: Information Security Risk Management V2.0

Guide to developing an Information Security Incident Management Framework V2.0

Information Sheet: Information Security Incident Notification Scheme V3.0

Department of Government Services:

IM-FW-01 Information Management Framework

IM-GUIDE-06 Information Management Governance Standards

https://www.vic.gov.au/information-management-policies-and-standards

Statement of Direction (**SOD**) – Workforce Identity and Access Management (**IDAM**)

https://www.vic.gov.au/identity-and-access-management-policies-and-standards

Victorian Government Cyber Incident Management Plan

https://www.vic.gov.au/cyber-incident-management-plan

Victorian Government Cyber Incident Response Plan Template

https://www.vic.gov.au/report-or-respond-cyber-incident

DataVic access policy guidelines

https://www.data.vic.gov.au/datavic-access-policy-guidelines

Department of Treasury and Finance:

Victorian Government Risk Management Framework (VGRMF)

https://www.dtf.vic.gov.au/victorian-risk-management-framework-and-insurance-management-policy

Victorian Managed Insurance Authority (VMIA):

Develop a foundation-level organisational framework

Embedding risk thinking and techniques

https://www.vmia.vic.gov.au/practical-guidance-managing-risk

Federal Government

Department of Home Affairs:

Protective Security Policy Framework (PSPF) Release 2025 and Guidelines 2025

https://www.protectivesecurity.gov.au/publications-library/pspf-annual-release-2025

https://www.protectivesecurity.gov.au/publications-library/pspf-guidelines-2025

National Identity Proofing Guidelines (NIPG) 2025

https://www.ag.gov.au/sites/default/files/2025-09/NIPG_report.pdf

Australian Signals Directorate (ASD) / Australian Cyber Security Centre:

Australian Government Information Security Manual (**ISM**)

https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism

ASD Essential Eight

https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight

Australian Standards

*Please note. For eligible Victorian Public Sector organisations, access to Australian Standards is free from the Victorian Government Library Service (**VGLS**).*

AS/NZS ISO/IEC 27001: 2023 Information security, cybersecurity and privacy protection - Information security management systems – Requirements

https://www.standards.org.au/standards-catalogue/standard-details?designation=as-nzs-iso-iec-27001-2023

AS/NZS ISO/IEC 27002: 2022 Information security, cybersecurity and privacy protection - Information security controls

https://www.standards.org.au/standards-catalogue/standard-details?designation=as-nzs-iso-iec-27002-2022

AS/NZS ISO/IEC 27005: 2024 Information security, cybersecurity and privacy protection — Guidance on managing information security risks

https://www.standards.org.au/standards-catalogue/standard-details?designation=as-nzs-iso-iec-27005-2024

AS ISO 31000: 2018 Risk Management - Guidelines

https://www.standards.org.au/standards-catalogue/standard-details?designation=as-iso-31000-2018

AS/NZS ISO/IEC 27035.1: 2025 Information technology - Information security incident management, Part 1: Principles and process

https://www.standards.org.au/standards-catalogue/standard-details?designation=as-nzs-iso-iec-27035-1-2025

AS/NZS ISO/IEC 27035.2:2025 Information technology - Information security incident management, Part 2: Guidelines to plan and prepare for incident response

https://www.standards.org.au/standards-catalogue/standard-details?designation=as-nzs-iso-iec-27035-2-2025

www.ovic.vic.gov.au