Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards

Version V2.0

Implementation Guidance V2.1

Victorian Protective Data Security Standards

Version 2.0 Implementation Guidance V2.1

Document details

Version	Publish date	Amendments in this version
1.0	June 2016	N/A
1.1	March 2018	Updated some control references
2.0	October 2019	Removed protocols Integrated elements including: a mapping to their primary control source 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 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E10.020, E10.050, E10.070 E11.030, E11.040, E11.090, E11.110, E11.120, E11.180 E12.010, E12.030, E12.040 Update outdated Appendix A links

Note. The issue of version 2.1 of this document does not represent a change to the Victorian Protective Data Security Standards V2.0. This document has been reviewed for currency and updated accordingly under the VPDSS product development cycle.

Victorian Protective Data Security Standards

Version 2.0 Implementation Guidance V2.1

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. The Standards are issued under Parts 4 and 5 of the *Privacy and Data Protection Act 2014*.

Objectives

The VPDSS is developed to help 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; and
- minimise 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)
Element	A security measure(s) extracted from the source reference point that provides high level guidance.	How to? (risk-based action)

VPDSS Structure	Description	Outcome
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.

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.

[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

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 ISO/IEC 27001:2015 Information security management systems - Requirements* § 4 § 5.2 § 6.2
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.	*AS ISO/IEC 27001:2015* § 4.2
E1.030	The organisation's information security management framework aligns with its risk management framework.	*AS ISO/IEC 27001:2015* § 6.1 *AS ISO/IEC 27005:2012 Information security risk management* § 5
E1.040	Executive management defines information security functions, roles, responsibilities, competencies, and authorities.	*AS ISO/IEC 27001:2015* § 5.3
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	*AS ISO/IEC 27001:2015* § 5.1

V2.0 #	Element	Primary Source
	plan.	
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.	*AS ISO/IEC 27001:2015* § 9
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).	*AS ISO/IEC 27001:2015* § 7.1 § 7.2
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.	*AS ISO/IEC 27001:2015* § 7.4
E1.100	The organisation documents its internal control library that addresses its information security risks.	*AS ISO/IEC 27001:2015* § 6.1
E1.110	The organisation monitors, reviews, validates, and updates the information security management framework.	*AS ISO/IEC 27001:2015* § 9.3 § 10.2

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.	*WoVG 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* § 9 § 10 § 11 § 12
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* § 12
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* § 6 § 7

V2.0 #	Element	Primary Source
E2.050	The organisation applies appropriate protective markings to information throughout its lifecycle.	*OVIC Practitioner Guide: Protective Markings* § 7 § 9 *Protective Security Policy Framework (PSPF) INFOSEC-8 Sensitive and Classified Information* § C.2.5
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* § 8.4
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* § 14
E2.080	The organisation manages externally generated information in accordance with the originator's instructions.	*OVIC Practitioner Guide: Protective Markings* § 19 - § 25
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) INFOSEC-8 Sensitive and Classified Information* § C.5.7 § C.5.7.1

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 *AS ISO/IEC 27005:2012 Information security risk management* § 8 § 9
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 *Victorian Government Risk Management Framework (VGRMF) Practice Guide* § Risk Process - Risk Register
E3.030	The organisation considers information security risks in organisational planning.	*VGRMF Practice Guide* § Risk Governance – Corporate and Business Planning

V2.0 #	Element	Primary Source
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 *AS ISO/IEC 27005:2012* § 11
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 *VGRMF* § 2.2.2 *VGRMF Practice Guide* § Risk Management - Risk Profile Review § Risk Process – Monitor and review *AS ISO/IEC 27005:2012* § 12.1 *AS ISO 31000:2018* § 6.7

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 ISO/IEC 27002:2015 Code of practice for information security controls* § 9.1.1 *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 ISO/IEC 27002:2015* § 9.2 *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 ISO/IEC 27002:2015* § 11.1.1 § 11.1.2

[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 ISO/IEC 27002:2015* § 9.1.2 § 9.2.1 § 9.4 *Australian Government Information Security Manual (ISM) Dec 2020* § Guidelines for Personnel Security – Access to systems and their resources *ACSC Essential Eight to ISM Mapping* § 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 ISO/IEC 27002:2015* § 9.2.2 *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 ISO/IEC 27002:2015* § 9.2.3 *SOD IDAM 01 – Workforce Identity and Access Management* § Privileged Access
E4.070	The organisation regularly reviews and adjusts physical and logical access rights taking into account operational changes.	*AS ISO/IEC 27002:2015* § 9.2.5 § 9.2.6

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).	*PSPF GOVSEC-2 Management structures and responsibilities* § C.8 *AS ISO/IEC 27002:2015 Code of practice for information security controls* § 7.1.2 § 7.2.1
E5.020	The organisation's information security training and awareness content covers all security areas.	*PSPF GOVSEC-2* § C.9.2
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 GOVSEC-2* § C.9 § C.9.3 *AS ISO/IEC 27002:2015* § 7.2.2
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 GOVSEC-2* § C.9 § C.9.1 § C.9.2

V2.0 #	Element	Primary Source
E5.050	The organisation reviews and updates the information security obligations of all persons with access to public sector information.	*AS ISO/IEC 27001:2015 Information security management systems - Requirements* § 10.2
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 GOVSEC-2* § C.9.3
E5.070	The organisation monitors, reviews, validates, and updates its information security training and awareness program and schedule.	*AS ISO/IEC 27002:2015* § 7.2.2

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 *AS ISO/IEC 27002:2015 Code of practice for information security controls* § 16.1.1 *PSPF GOVSEC-2 Management structures and responsibilities* § C.7 *Victorian Government cyber incident response plan template*
E6.020	The organisation articulates roles and responsibilities for information security incident management.	*ISIMF* § A *AS ISO/IEC 27002:2015* § 16.1.1

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 ISO/IEC 27035.1:2017 Information security incident management Part 1: Principles of incident management* § 5 *ISIMF* § A *WoVG Cyber Incident Management Plan* § Managing Cyber Incidents *AS ISO/IEC 27002:2015* § 16.1.1 *PSPF GOVSEC-2* § Annex A
E6.040	The organisation records information security incidents in a register.	*PSPF GOVSEC-2* § C.7.1.3 § Annex A Step 1 *AS ISO/IEC 27035.2:2017 Information security incident management Part 2: Guidelines to plan and prepare for incident response* § Annex B.2.2
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.	*PSPF GOVSEC-2* § C.7.2 § Annex B

V2.0 #	Element	Primary Source
E6.060	The organisation regularly tests (e.g., annually) its incident response plan(s).	*AS ISO/IEC 27035.2:2017* § 11 *WoVG Cyber Incident Management Plan* § Managing Cyber Incidents *WoVG Cyber Exercise Guide*

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 ISO/IEC 27002:2015 Code of practice for information security controls* § 17.1.1
E7.020	The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans.	*AS ISO/IEC 27002:2015* § 17.1.2
E7.030	The organisation regularly tests (e.g., annually) its business continuity and disaster recovery plan(s).	*AS ISO/IEC 27002:2015* § 17.1.3

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 ISO/IEC 27002:2015 Code of practice for information security controls* § 13.2.1 § 15.1.1
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.	*PSPF GOVSEC-6 Security governance for contracted service providers* § C.2 *PSPF INFOSEC-9 Access to information* § C.1 *AS ISO/IEC 27002:2015* § 13.2.2 § 13.2.4 § 15.1.2
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 GOVSEC-6* § C.1 § C.3.1

V2.0 #	Element	Primary Source
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 ISO/IEC 27002:2015* § 6.1.1 (e)
E8.050	The organisation establishes, maintains, and reviews a register of third-party arrangements (e.g., contracts, MOUs and information sharing agreements).	*AS ISO/IEC 27002:2015* § 15.1.1
E8.060	The organisation monitors, reviews, validates, and updates the information security requirements of third-party arrangements and activities.	*PSPF GOVSEC-6* § C.3 *AS ISO/IEC 27002:2015* § 15.2.1 *PDP Act* § 89 (3)
E8.070	The organisation documents its information release management requirements (e.g., social media, news, DataVic).	*IM-GUIDE-06 WoVG Information Management Governance Guidelines* § *Custodianship model*
E8.080	The organisation manages the delivery of maintenance activities and repairs (e.g., on-site, and off-site).	*AS ISO/IEC 27002:2015* § 11.2.4 *ISM Dec 2020* § Guidelines for ICT equipment–ICT 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 GOVSEC-6* § C.4

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.[4]	*OVIC Information Security Incident Notification Scheme V1.0*
E9.020	The organisation submits its Protective Data Security Plan (PDSP) to OVIC every two years.	*Privacy and Data Protection Act 2014* (PDP Act) § 89 4 (b)
E9.030	Upon significant change, the organisation submits its reviewed PDSP to OVIC.	*PDP Act* § 89 4 (a)
E9.040	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.	*VPDSF V2.0* § 9.3

[4] Refer to the current VPDSF BIL table on the OVIC website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-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).	*PSPF GOVSEC-2 Management structures and responsibilities* § C.6 *PSPF GOVSEC-3 Security planning and risk management* § C.2 Table 2 *PSPF PERSEC-13 Ongoing assessment of personnel* § C.1 Table 1 *PSPF PERSEC-14 Separating personnel* § C
E10.020	The organisation verifies the identity of personnel, re-validates, and manages any changes as required.	*PSPF PERSEC-12 Eligibility and suitability of personnel* § para 11 Table 1 Identity checks § C.3.4 Table 4 Confirmation of identity *National Identity Proofing Guidelines (NIPG)* § 4.1
E10.030	The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.	*PSPF PERSEC-12* § C.1

V2.0 #	Element	Primary Source
E10.040	The organisation manages ongoing personnel eligibility and suitability requirements commensurate with its security and probity obligations and risk profile.	*PSPF PERSEC-13* § C.1
E10.050	The organisation manages personnel separating from the organisation commensurate with its security and probity obligations and risk profile.	*PSPF PERSEC-14* § C.1 - § C.6
E10.060	The organisation develops security clearance policies and procedures to support roles requiring high assurance and/ or handling security classified information.	*PSPF PERSEC-13* § C.1 Table 1
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 PERSEC-12* § C.2
E10.080	The organisation actively monitors and manages security clearance holders.	*PSPF PERSEC-13* § C.2

Standard 11 – Information Communications Technology (ICT) Security

Standard

An organisation establishes, implements and maintains Information Communications Technology (ICT) 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) Dec 2020* § Guidelines for 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 ICT 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
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 *ACSC Essential Eight to ISM Mapping* § Patch applications § Patch Operating Systems
E11.050	The organisation documents and manages changes to ICT systems.	*ISM* § Guidelines for system management – Change management

V2.0 #	Element	Primary Source
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 – wireless devices and radio frequency transmitters
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
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 *ACSC Essential Eight to ISM Mapping* § Application Control § Configure Microsoft Office macro settings § 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 - Using Network-based Intrusion Detection and Prevention Systems

V2.0 #	Element	Primary Source
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 *ACSC Essential Eight to ISM Mapping* § 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
E11.140	The organisation manages a process for cryptographic keys (e.g., disk encryption, certificates).	*AS ISO/IEC 27002:2015 Code of practice for information security controls* § 10.1.2
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
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

V2.0 #	Element	Primary Source
E11.180	The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing, retention).	*ISM* § Guidelines for system management *ACSC Essential Eight to ISM Mapping* § Daily 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
E11.200	The organisation manages security measures for enterprise mobility (e.g., mobile device management, working from home).	*ISM* § Guidelines for enterprise mobility *AS ISO/IEC 27002:2015* § 6.2 *PSPF PHYSEC-15 Physical security for entity resources* § C.8

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.	*PSPF PHYSEC-16 Entity facilities* § C.1
E12.020	The organisation applies defence-in-depth physical security measures.	*Victorian Government Office Accommodation guidelines* § 2.6 § 4.7 *PSPF PHYSEC-16* § C.2 § C.4 *AS ISO/IEC 27002:2015 Code of practice for information security controls* § 11.1

V2.0 #	Element	Primary Source
E12.030	The organisation selects physical security measures commensurate with the business impact level of the information.	*Victorian Government Office Accommodation guidelines* § 4.7 *PSPF PHYSEC-15 Physical security for entity resources* § C.2 § C.3 *PSPF PHYSEC-16* § C.2 § C.3 *AS ISO/IEC 27002:2015* § 11.2
E12.040	The organisation has scalable physical security measures ready for activation during increased threat situations.	*PSPF GOVSEC-3 Security planning and risk management* § C.3 *PSPF PHYSEC-16* § C.4
E12.050	The organisation implements physical security measures when handling information out of the office.	*PSPF PHYSEC-15* § C.8 *AS ISO/IEC 27002:2015* § 11.2.6
E12.060	The organisation manages physical security measures throughout their lifecycle.	*AS ISO/IEC 27002:2015* § 11.2.4 § 11.2.7

Appendix A - VPDSS Primary Sources

Victorian Government

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

http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/vic/consol_act/padpa2014271/

Office of the Victorian Information Commissioner:

Victorian Protective Data Security Framework (**VPDSF**) V2.0

Practitioner Guide: Identifying and Managing Information Assets

Practitioner Guide: Assessing the security value of public sector information

Practitioner Guide: Protective Markings

Practitioner Guide: Information Security Risk Management

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

https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

Information Security Incident Notification Scheme V1.0

https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/

Enterprise Solutions Branch:

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 – Workforce Identity and Access Management

https://www.vic.gov.au/digital-strategy-transformation-statements-direction

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/prepare-cyber-incident

Cyber Exercise Guide

https://www.vic.gov.au/practice-your-cyber-incident-response

Department of Treasury and Finance:

Victorian Government Risk Management Framework (**VGRMF**)

https://www.dtf.vic.gov.au/planning-budgeting-and-financial-reporting-frameworks/victorian-risk-management-framework-and-insurance-management-policy

Victorian Government Office Accommodation guidelines

https://www.dtf.vic.gov.au/shared-service-provider/office-accommodation-guidelines

*Victorian Managed Insurance Authority (**VMIA**):*

VGRMF Practice Guide

https://www.vmia.vic.gov.au/tools-and-insights/tools-guides-and-kits/victorian-government-risk-management-framework

Federal Government

Attorney-General's Department:

Protective Security Policy Framework (**PSPF**) -

GOVSEC-2 Management structures and responsibilities

https://www.protectivesecurity.gov.au/governance/management-structures-and-responsibilities/Pages/default.aspx

GOVSEC-3 Security planning and risk management

https://www.protectivesecurity.gov.au/governance/security-planning-risk-management/Pages/default.aspx

GOVSEC-6 Security governance for contracted goods and service providers

https://www.protectivesecurity.gov.au/governance/security-governance-for-contracted-service-providers/Pages/default.aspx

INFOSEC-8 Sensitive and classified information

https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx

INFOSEC-9 Access to information

https://www.protectivesecurity.gov.au/information/access-to-information/Pages/default.aspx

PERSEC-12 Eligibility and suitability of personnel

https://www.protectivesecurity.gov.au/personnel/eligibility-and-suitability-of-personnel/Pages/default.aspx

PERSEC-13 Ongoing assessment of personnel

https://www.protectivesecurity.gov.au/personnel/ongoing-assessment-of-personnel/Pages/default.aspx

PERSEC-14 Separating personnel

https://www.protectivesecurity.gov.au/personnel/separating-personnel/Pages/default.aspx

PHYSEC-15 Physical security for entity resources

https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx

PHYSEC-16 Entity Facilities

https://www.protectivesecurity.gov.au/physical/entity-facilities/Pages/default.aspx

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

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

https://www.cyber.gov.au/acsc/view-all-content/ism

ACSC Essential Eight

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

Home Affairs:

National Identity Proofing Guidelines (**NIPG**)

https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-security

Australian Standards

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

AS ISO/IEC 27001: 2015 Information technology - Security techniques - Information security management systems – Requirements

https://www.standards.org.au/standards-catalogue/sa-snz/communication/it-012/as--iso-slash-iec--27001-colon-2015

AS ISO/IEC 27002: 2015 Information technology - Security techniques - Code of practice for information security controls

https://www.standards.org.au/standards-catalogue/sa-snz/communication/it-012/as--iso-slash-iec--27002-colon-2015

AS ISO/IEC 27005: 2012 Information technology - Security techniques – Information security risk management

https://www.standards.org.au/standards-catalogue/sa-snz/communication/it-012/as-slash-nzs--iso-slash-iec--27005-2012

AS ISO 31000: 2018 Risk Management - Guidelines

https://www.standards.org.au/standards-catalogue/sa-snz/publicsafety/ob-007/as--iso--31000-colon-2018

AS ISO/IEC 27035.1: 2017 Information technology - Security techniques – Information security incident management, Part 1: Principles of incident management

https://www.standards.org.au/standards-catalogue/sa-snz/communication/it-012/as--iso-slash-iec--27035-dot-1-colon-2017

AS ISO/IEC 27035.2:2017 Information technology - Security techniques – Information security incident management, Part 2: Guidelines to plan and prepare for incident response

https://www.standards.org.au/standards-catalogue/sa-snz/communication/it-012/as--iso-slash-iec--27035-dot-2-colon-2017