VPDSS Standard 1 – Security Management Framework

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

VPDSS Control Reference Descriptors - AS/NZS 27001

VPDSS Elements
SMF-010 Organisations have a documented, contextual information security management framework.
SMF-020 The information security management framework contains and references all legislative and regulatory drivers.
SMF-030 Executive endorse and sponsor protective data security.
SMF-040 Executive have defined protective data security functions, roles, responsibilities, competencies and authorities.
SMF-050 Organisations refer to the risk management framework in the information security management framework.
SMF-060 Executive have established and communicated an information security strategy and implementation plan.
SMF-070 Executive have committed to providing sufficient resources to support protective data security.
SMF-080 The information security management framework is sufficiently communicated and accessible.
SMF-090 Organisations monitor, review, validate and update the information security management framework.

VPDSS Standard 2 – Security Risk Management

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

VPDSS Control Reference Descriptors - AS/NZS 31000, VGRMF, HB167

VPDSS Elements
SRM-010 Organisations have incorporated security into their risk management framework.
SRM-020 Organisations conduct security risk profile assessments to identify risks to information assets.
SRM-030 The organisation's risk register has a record of identified security risks.
SRM-040 Security risks are included in organisational planning.
SRM-050 Organisations collaborate with internal and external stakeholders during the security risk management process.
SRM-060 Organisation's security risk profile is regularly reviewed.
SRM-070 Organisations govern, monitor, review and report on security risk through an audit committee.

VPDSS 3 – Security policies and procedures

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

VPDSS Control Reference Descriptors - PSPF Better practice guide Developing agency protective security policies plans and procedures v1.1

VPDSS Elements
SPP-010 Organisation's policies and procedures cover governance arrangements and the security domains of information, personnel, ICT and physical.
SPP-020 Organisational protective data security documentation contains controls to manage risk.
SPP-030 Executive approve information security policies.
SPP-040 Organisations monitor, review, validate and update security policies and procedures.

VPDSS Standard 4 – Information Access

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

VPDSS Control Reference Descriptors - ISO/IEC 27002:2013, National e-Authentication Framework, NIST Special publication 800-53

VPDSS Elements
IAM-010 Organisations have an identity and access management policy.

IAM-020 Organisations have a process for managing identities and the issuance of secure credentials for physical and logical access.

IAM-030 Organisations track access to and use of, key official information.

Physical access to information

IAM-040 Organisations have physical access controls.

Electronic access to information

IAM-050 Organisations have logical access controls.

IAM-060 Organisations follow documented access registration and de-registration processes.

IAM-070 Organisations follow documented access provisioning and de-provisioning processes.

IAM-080 Organisations actively manage privileged access accounts and ensure separation from normal access accounts.

VPDSS Standard 5 – Security obligations of all people with access to public sector data

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

VPDSS Control Reference Descriptors - Protective Security Guidelines - Agency Personnel Security Responsibilities & Australian Government Personnel Security Protocol of the Protective Security Policy Framework (PSPF).

VPDSS Elements

SOP-010 Organisations identify, document and communicate personnel security obligations.

SOP-020 Personnel are regularly reminded of their security obligations and reaffirm their agreement to meet these obligations.

SOP-030 Organisations monitor, review, validate and update their personnel security obligations.

VPDSS Standard 6 – Security Training and Awareness

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

VPDSS Control Reference Descriptors - Protective Security Guidelines - Agency Personnel Security Responsibilities & Australian Government Personnel Security Protocol of the Protective Security Policy Framework (PSPF).

VPDSS Elements

STA-010 Organisation's training policies and procedures include security training and awareness.

STA-020 Security training and awareness is delivered to all persons, upon engagement and regular intervals thereafter.

STA-030 Security training and awareness covers all protective data security domains.

STA-040 Organisations provide targeted training to personnel in high risk roles or who have role specific security obligations

STA-050 Security training and awareness is supported by security awareness programs.

STA-060 Organisations monitor, review, validate and update security training and awareness programs.

VPDSS Standard 7 – Security Incident Management

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

VPDSS Control Reference Descriptors - 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).

VPDSS Elements

SIM-010 Organisations have security incident management policies and procedures covering all protective data security domains.

SIM-020 Organisations articulate roles and accountabilities of personnel involved in security incident management.

SIM-030 Security incident management procedures are underpinned by a communications plan.

SIM-040 Security incident management policies and procedures contain the five phases of:
* Plan and prepare
* Detect and report
* Assess and decide
* Respond
* Lessons learnt

SIM-050 Organisations have a register of all security incidents.

SIM-060 Security incident management procedures identify and categorise administrative vs criminal incidents and investigative handover.

SIM-070 Organisations monitor and review security incidents and investigations to validate and update security incident management procedures and activities.

VPDSS 8 – Business continuity management
An organisation must establish, implement and maintain a business continuity management program that addresses the security of public sector data.

VPDSS Control Reference Descriptors - AS 5050:2010 Business Continuity - managing disruption-related risk - ISO 22301:2012 Societal Security - Business Continuity management systems - requirements - ANAO better practice guide Business continuity management - Building resilience in public sector entities

VPDSS Elements
BCM-010 All protective data security domains are represented in the business continuity management policy and plans.
BCM-020 Organisations identify and assign roles and responsibilities for protective data security in business continuity policies and plans.
BCM-030 Organisations include protective data security requirements in their BCP communications plan.
BCM-040 Organisations monitor, review, validate and update the protective data security requirements of their BCP.

VPDSS 9 – Contracted Service Providers
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).

VPDSS 10 – Government Services
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.

VPDSS Control Reference Descriptors - PSPF Security of outsourced services and functions
https://www.protectivesecurity.gov.au/governance/contracting/Documents/Security-of-outsourced-services-and-functions-guidelines.pdf and
ANAO Developing and Managing Contracts
https://www.anao.gov.au/sites/g/files/net1661/f/2012_Developing_And_Managing_Contracts_BPG.pdf

VPDSS Elements
SUP-010 Organisations have documented procedures and controls covering the entire lifecycle of supplier management.
SUP-020 Requirements from all protective data security domains are included in service arrangements.
SUP-030 Security controls to be included in service arrangements are assessed in the supplier's environment before finalising arrangements.
SUP-040 Information assets and supplier security controls are transitioned at cessation of the supplied service.
SUP-050 Organisations identify and assign protective data security roles and responsibilities in service arrangements.
SUP-060 Protective data security is embedded in procurement policy and procedures.
SUP-070 Organisations monitor, review, validate and update the security requirements of service arrangements.

VPDSS Standard 11 – Security Plans
An organisation must establish, implement and maintain a protective data security plan to manage their security risks.

VPDSS Control Reference Descriptors - AS/NZS 31000, VGRMF, HB167

VPDSS Elements
RTP-010 Security risks inform organisational planning.
RTP-020 Organisations have a documented and approved protective data security plan (PDSP).
RTP-030 Risk treatments are assigned to owners with accountability for implementation, monitoring, evaluation and review.

VPDSS 12 – Compliance
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.

VPDSS Control Reference Descriptors - AS ISO 19600:2015 Compliance Management Systems - Guidelines

VPDSS Elements
COM-010 Organisations identify and manage the risks from any protective data security non-compliance.

COM-020 Organisations monitor protective data security compliance obligations and identify performance indicators.

COM-030 Organisations report on their compliance obligations with protective data security.

COM-040 Organisations independently audit protective data security compliance obligations.

VPDSS 13 – Information Value

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

VPDSS Control Reference Descriptors - Information Security Guide - Chapter 1 - Understanding Information Value

VPDSS Elements
INF-010 Organisations have defined their information asset types.
INF-020 Organisations have conducted an information review to identify their information assets in consultation with their internal stakeholders.
INF-030 Organisations have identified and documented the security attributes of their information assets.
INF-040 Organisations have established and manage an information asset register.
INF-050 Organisations have identified accountable roles for assets in their information asset register.
INF-060 Organisations use a contextualised VPDSF business impact level table to value official information.
INF-070 Organisations have identified the aggregated value of official information.
INF-080 Organisations continually review the value of official information across its lifecycle.

VPDSS 14 – Information Management

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

VPDSS Control Reference descriptor - VPDSF Information Security Guide: Chapter 2 – Protective Markings, WoVG Information Management Principles and the Public Record Office of Victoria (PROV) Standards and Policies. DataVic Access Policy and the information controls contained in the Information Security Management Protocol of the Protective Security Policy Framework (PSPF).

VPDSS Elements
INM-010 The organisation's Information Management Framework incorporates all protective data security domains.
INM-020 Organisations monitor, review, validate and update references to protective data security domains in their Information Management Framework.
Information lifecycle
INM-030 Organisations handle official information commensurate with it's value throughout its lifecycle.
INM-040 Organisations apply appropriate protective markings to information throughout its lifecycle.

VPDSS 15 – Information Sharing

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

VPDSS Control Reference Descriptor - ISO/ IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls [Information transfer].

VPDSS Elements
INS-010 The organisation's information sharing procedures cover all the protective data security domains.
INS-020 Information sharing agreements include protective data security requirements.
INS-030 Security controls to be included in information sharing agreements are assessed in the receiving organisation's environment before finalising agreements.
INS-040 Organisations establish, maintain and review a register of information sharing agreements.
INS-050 Organisations monitor, review, validate and update the security requirements of information sharing agreements.

VPDSS 16 – Personnel Lifecycle

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

VPDSS Control Reference Descriptors - 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)

VPDSS Elements
PER-010 Organisation's human resources management policies and procedures identify personnel security measures.
PER-020 Organisations verify and manage the identity of personnel throughout the engagement lifecycle.
PER-030 Organisations undertake pre-engagement screening commensurate with their security obligations and risk profile.
PER-040 Organisations manage ongoing personnel eligibility and suitability requirements.
PER-050 Organisation's personnel security policies and procedures address the personnel lifecycle phases of: * Pre-engagement * Engagement * Post engagement

Additional controls for organisations requiring security clearances

PER-060 Organisations with roles handling security classified information or requiring high assurance develop security clearance policies and procedures.
PER-070 Organisations with roles handling security classified information or requiring high assurance undertake additional personnel screening measures commensurate with the risk.
PER-080 Organisations actively monitor and manage security clearance holders.

VPDSS 17 – ICT Security

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

VPDSS Control Reference Descriptors - Australian Signals Directorate Information Security Manual http://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf

VPDSS Elements
ICT-010 Organisations have security documentation for ICT systems.
ICT-020 Organisations manage all ICT assets throughout their lifecycle.
ICT-030 Organisations have disaster recovery plans for ICT systems.
ICT-040 Organisations have an ICT system accreditation framework for systems transmitting, processing or storing security classified information.
ICT-050 Organisations manage vulnerabilities to their ICT systems throughout the ICT system lifecycle.
ICT-060 Organisations document and manage changes to ICT systems.
ICT-070 Organisations have communications security controls.
ICT-080 Organisations verify the vendors security claims before implementing security technologies.
ICT-090 Organisations have security measures (classification, labelling, usage, sanitisation, destruction, disposal) in place for media.
ICT-100 Organisations have hardened standard operating environments (SOEs) for workstations and servers commensurate with security risk.
ICT-110 Organisations have security measures for email use.
ICT-120 Organisations have system logging and monitoring to record events.
ICT-130 Organisations have secure administration practices.
ICT-140 Organisations have designed and configured the ICT network in a secure manner.
ICT-150 Organisations use cryptographic controls for confidentiality, integrity, non-repudiation and authentication commensurate with the risk to information.
ICT-160 Organisations have a cryptographic policy governing key management.
ICT-170 Organisations have malware prevention and detection software installed on all ICT systems.
ICT-180 Organisations have a capacity management system.
ICT-190 Organisations have separated development, testing and production environments.
ICT-200 Organisations have a backup management system.
ICT-210 Organisations have a secure development lifecycle.

VPDSS 18 – Physical lifecycle

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

VPDSS Control Reference Descriptors - PSPF - Physical security management protocol;

VPDSS Elements
PHY-010 Organisation's facilities and building management policies and procedures include physical security measures.

PHY-020 Organisations apply defence-in-depth physical security layers in the protection of information.
PHY-030 Organisations include physical security measures as part of their site selection, build or refurbishment procedures.
PHY-040 Organisations document security measures associated with their security zones.
PHY-050 The organisation selects security equipment and services commensurate with the business impact level of the information and the security zone of the facility/environment.
PHY-060 Organisations have scalable physical security measures ready for activation during increased threat situations.
PHY-070 Organisations manage the physical security of their information and information systems when handled out of the office.
PHY-080 Organisations manage physical security equipment and services throughout their lifecycle.
PHY-090 Organisations monitor, review, validate and update physical security measures.