Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards - Glossary

Version 2.0 November 2019

Document Details

Victorian Protective Data Security Standards Glossary	
Protective Marking	N/A
Approved for unlimited public release	*Yes – Authorised for release*
Release Date	November 2019
Review Date	November 2020
Document Version	2.0
Authority	Office of the Victorian Information Commissioner (OVIC)
Author	Information Security Unit – OVIC

For further information, please contact the Information Security Unit on security@ovic.gov.au

Version	Publish date	Amendments in this version
1.0	June 2016	N/A
2.0	November 2019	• Changed branding from CPDP to OVIC • Added new terms: ○ All persons ○ Community of practice ○ Control environment ○ Cyber security ○ Defence-in-depth ○ Element(s) ○ High assurance ○ Impact statements ○ Information asset ○ Information Management Markers ○ Information release ○ Information security ○ Information security value assessment ○ Internal control library ○ Personnel ○ Public sector information ○ Primary source ○ Risk register ○ Security areas ○ Security attributes ○ Security maturity ○ Security value

		○ Significant change ○ Statement of Applicability ○ Third party • Removed terms no longer in use: ○ Consequences ○ Official information ○ Protocol(s) ○ Regime ○ Security domains ○ Valuation criteria

Term	Definition
Agency	As per PDPA, a public service body (departments and administrative offices) or a public entity (a body established under an Act, by the Governor in Council or by a Minister) within the meaning of the Public Administration Act 2004.
Aggregation	A compilation of information. Compilations of public sector information may require enhanced protection, as the combination of the information assets may be a greater value than any single part.
Agreement	A formal and legally binding contract between the State and a third party or parties. For example, a contract between a VPS organisation, on behalf of the State, and a third-party company delivering IT services. State agreements are usually in writing.
All persons	Employees, volunteers, contractors / sub-contractors and consultants, whether directly or indirectly engaged by the organisation with access to public sector information. Also referred to as Personnel.
Arrangement	An informal and non-legally binding understanding between the State and a third party. A memorandum of understanding between two parts of the State is also an arrangement because it is not possible to make a legally binding contract between two parts of the same legal entity – the State of Victoria.
Asset	Any item (whether tangible or intangible) that has a useful or valuable quality for an organisation. This includes information, physical and personnel assets to support that organisation's business functions, services and activities. Value can be subjective or objective.
Availability	The desired state that allows authorised persons to access defined information for authorised purposes at the time they need to do so.

Body	A body that is a special body, within the meaning of section 6 of the Public Administration Act 2004 and a body declared by the Governor in Council by Order published in the Government gazette to be a body to which Part Four applies. The entity can be incorporated or not. *Incorporated* – An organisation that exists as a separate legal entity in its own right. *Unincorporated* – An association or body which exists legally only through those who belong to the association. A partnership is an example of an unincorporated association.
Business Impact Level (BIL)	Scaled impacts which would cause harm or damage to government operations, organisations or individuals, if there were a compromise of the confidentiality, integrity and/or availability of public sector information.
Caveat	A warning that the information has special requirements in addition to those indicated by a security classification. Certain information (most notably some information impacting on national security) may bear a caveat in addition to a security classification. Caveats are not classifications in their own right and must be used in conjunction with a security classification. They cannot be applied to 'Unofficial' information.
Community of Practice	An organised group of people who share common interests, passions or concerns for something they do, collaborating together to resolve issues, improve skills, share knowledge and learn from each other's experiences.
Confidentiality	The limiting of public sector information to authorised persons for approved purposes. The confidentiality requirement is determined by considering the potential impacts of unauthorised disclosure of the public sector information.
Contracted service provider	A person or body who provides services under a State contract. Contracted service providers are also referred to as outsourced service providers.

Control(s)	Baseline or minimum expected measures representing better practice.
Control environment	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.
Critical assets	Essential or important assets, which if compromised, degraded, rendered unavailable for an extended period or destroyed, would significantly impact on the social or economic wellbeing of the organisation or Victorian community.
Critical services	Either essential or important Government services. The compromise to the confidentiality, integrity or availability of these services would result in serious damage to the physical, social or economic wellbeing of the State of Victoria. The context for these services is the prevention, or management of, a disaster or crisis.
Cyber security	Measures relating to the confidentiality, integrity, availability of information and data that is processed, stored and communicated by electronic or similar means, protecting it and associated systems from external or internal threat.
Data	Refer to '*public sector data*'
Declassify	The process of re-assessing the security value of public sector information and downgrading an existing protective marking to a lesser protective marking.
Defence-in-depth	A multi-layered system in which security measures combine to make it difficult for 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.

Dissemination Limiting Marker (DLM)	A protective marking that indicates access to and of the information should be restricted. This may be due to legislative enactments or provisions that limit access or disclosure, or where special handling is required, and subsequent dissemination of the information needs to be controlled.
Element(s)	An element is security measure that modifies risk. Elements often depend on a supportive control environment to be effective. Also referred to as VPDSS Elements
Functional equivalents	Alternative security measure that provide the same or better functionality as the specified control. An exception is not required in this instance. N.B. Before agreeing to the use of alternative protective security measures a public sector body Head, must seek expert advice to confirm that the technical performance requirements of the proposed measures meet or exceed those of the specified control.
Government services	Organisations (public or private) undertaking a specific role on behalf of the government for the government.
Guides	Detailed set of instructions and/or guidance material, with regard to a set process or practice. Under the VPDSF guides are also referred to as security guides or sec guides.
High assurance	Roles/positions within organisations that have high levels of privilege and or influence associated with their role (e.g. credit controllers, system administrators, senior executives). These roles/positions may not necessarily have access to security classified information, but have the ability to influence important organisational outcomes and management of public sector information.
Impact statements	The effect, result or outcome of something occurring from a compromise of public sector information. A natural or logical outcome from an action or condition.
Impact category	Grouping of like 'impacts' that are derived from a similar family/ topic.

Impact level(s)	Potential impacts describing the degree to which a compromise of the information is likely to cause harm or damage. These levels are scaled – commencing at zero and scaling to a maximum of four under the VPDSF Business Impact Levels (BILs).
Information asset	A body of information, defined and practically managed so it can be understood, shared, protected and used to its full potential. Information assets support business processes and are stored across a variety of media and formats (i.e. both paper-based as well as electronic material). Information assets have a recognisable and manageable value, risk, content and lifecycle.
Information Communications Technology (ICT) system lifecycle	A concept that addresses all phases of its existence to include system conception, design and development, production and/or construction, distribution, operation, maintenance and support, retirement, phase-out and disposal. It takes into account the systems development life cycle (SDLC), which considers the process of planning, creating, testing and deploying ICT systems.
Information lifecycle	The use and management of public sector information from cradle to grave. This includes the management of information from identification, creation, receipt, collection, dissemination, exchange, maintenance and preservation through to disposal (either archived or destroyed).
Information management	The way in which an organisation plans, identifies, creates, receives, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains, preserves and disposes of its information. It is also the means through which the organisation ensures that the value of that information is identified and used to its full potential.

Information Management Markers (IMMs)	Reflect 'rights properties' for particular content and can inform access restrictions. They act as metadata indicators that provide a standard set of terms ensuring common understanding and consistency where access or disclosure of information is to be limited as: • disclosure of the material is limited or prohibited by legislation; • special handling of the material is required; and • dissemination of the material needs to be controlled.
Information owner	A nominated role or entity responsible for the secure management of all information under their control, on behalf of the owning organisation.
Information release	Where an organisation authorises the uncontrolled dissemination of their information, or publication. Prior to undertaking an information release, organisations should conduct a risk assessment.
Information security	A risk management process designed to safeguard information assets and systems in a way that is proportionate to threats and supportive of business outcomes. It uses a combination of procedural, physical, personnel, information and ICT security measures designed to provide government (organisations) information, functions, resources, employees and clients with protection against security threats. Also referred to as data protection or protective data security.
Information Security Management Framework (ISMF)	Organisationally defined guiding principles that set the boundaries of behaviours for using its information, assets and resources. The core focus of the framework defines the organisation's risk tolerance, which suggests the range of security events the organisation is prepared to withstand.

Information security value assessment	A method to assess information to determine the overall security value of the content. The assessment process involves three core stages: 1. review the content; 2. consider potential impacts if the information was compromised; 3. understand the overall security value of the information, in order to apply the appropriate security measures.
Information sharing	Where the information owner specifies security measures that a receiving organisation must implement and maintaining, in order to provide a level of assurance.
Integrity	Assurance that public sector information has been created, amended or deleted only by the intended authorised means and is correct and valid.
Internal control library	Collection of documented specific security measures as selected by the organisation.
Legacy information	Public sector information that has been protectively marked under a former protective marking or security classification scheme (e.g. Protective Security Manual [PSM], Whole of Victorian Government [WoVG] SEC STD's).

National interest	A matter which has or could have impact on Australia, including:
	• national security;
	• international relations;
	• law and governance, including:
	  ○ State / territory relations
	  ○ law enforcement operations where compromise could hamper or prevent national crime prevention strategies or investigations or endanger personal safety
	• economic wellbeing;
	• heritage; or
	• culture.

Organisation	The collective term for Victorian public sector organisations, defined as an 'applicable' agency or body under section 84 of the PDPA.
Originator	The person, or organisation, responsible for preparing / creating public sector information or for actioning information generated outside the public sector (i.e. private industry). This person, or organisation, is also responsible for deciding whether, and at what level, to value / protectively mark that public sector information.
Personnel security	The management of personnel across the following phases: • Pre-engagement (eligibility and suitability); • Engagement (ongoing and re-engagement); and • Separating (permanently or temporarily).
Physical security	The management of a secure environment addressing facilities, equipment and services designed to prevent unauthorised access to public sector resources and to detect and respond to intruders. This includes planning, selection, building, and modification through to disposal of assets and facilities, or retirement of services.

Primary Source	Reference point where the element has been primarily derived from, for further implementation advice. References include Australian and International Standards, Federal and State government guidance and tailored guides developed by OVIC.
Protective data security	Refer to *Information Security*
Protective Data Security Plan (PDSP)	As required under section 89 of the PDPA. A formal endorsed document that consists of the actions to address security risks and improve protective data security of the agency or body, including the mitigation of identified risks and improvement of protective data security capability. It acts as a roadmap outlining how the organisation addresses or intends to address information security risks and implement the Standards. This plan is directly informed by the treatment of risks assessed and gaps in the implementation of the standards identified in a self-assessment.
Protective data security standards	Refer to *Victorian Protective Data Security Standards (VPDSS)*
Protective marking(s)	A security label assigned to public sector information. It signifies the confidentiality requirements of public sector information, determined via an information security value assessment based on the VPDSF Business Impact Level (BIL) table. Protective markings inform the minimum level of protection to be provided throughout the information lifecycle (e.g. during the use, storage, transmission/transfer and disposal).
Protective security	A combination of procedural, physical, personnel, ICT and information measures designed to protect public sector assets (information, functions, resources, people) from security threats.
Public sector body Head	The head of any Victorian Government department, authority, agency or body identified as an applicable organisation under Part Four of the PDPA 2014

Public sector data	Any information (including personal information) obtained, received or held by an agency or body to which Part 4 applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body. Also referred to as public sector information.
Public sector information	Refer to *public sector data*.
Public sector organisations	A collective term to cover Victorian public sector agencies and bodies
Resources	Supporting material under the VPDSF, to assist with the implementation of the Standards. Resources include practitioner guides, information sheets, reference material, templates, working examples, ready reckoners, visuals, etc.
Risk appetite	As derived from the Victorian Government Risk Management Framework, "The type and amount of risk that an agency is prepared to accept or avoid."
Risk posture	An organisation's overall risk position, that is, current business and strategic risks being managed.
Risk profile	Refer to *security risk profile*.
Risk register	A record of the results of risk assessments and treatment plans. This may take the form of a document, spreadsheet, software application.
Risk tolerance	As derived from the Victorian Government Risk Management Framework, "The agency's readiness to bear the risk after risk treatment in order to achieve objectives. Risk tolerances are based on the maximum level of acceptable risk and may be expressed in various ways depending on the nature of the risk."
Security	The preparedness, protection and preservation of people, property and information both tangible and intangible (from threat).

Security by Design (SbD)	A methodology that enables security to be 'built in' to the design and architecture of information systems and business processes. SbD aims to ensure that security is considered before and throughout the development and implementation of initiatives that involve the collection and handling of information. It involves a level of intentionality regarding security management.
Security areas	Formerly referred to as a *Security Domains.* Refers to key areas or disciplines of information, Information Communications Technology (ICT), personnel and physical security N.B. governance is not traditionally recognised as a core security area but is an essential component of the VPDSS.
Security attributes	Refers to the confidentiality, integrity and availability requirements of public sector information.
Security classification	Public sector information that has been security assessed as having a business impact level of 2, (high) or above for potential compromise of its confidentiality. This results in a security classification as a protective marking. Security classifications include PROTECTED, SECRET and TOP SECRET.
Security maturity	The degree of formality and optimisation of processes, from ad hoc practices, to formally defined steps, to managed result metrics, to active optimisation of the processes.
Security measures	A policy, procedure or technical solution for the mitigation of security risks and protection of information.
Security risk profile	A description of any set of security risks for an agency or body. These can relate to the whole organisation or part of the organisation.
Security Risk Profile Assessment (SRPA)	As required under section 89 of the PDPA. A process that organisations undertake to assess and manage information security risks.
Security value	The highest overall business impact of the public sector information, based on a holistic assessment of compromise to the confidentiality, integrity and or availability.

Sensitivity	An assessment outcome (using the BILs) that considers compromise to the confidentiality of public sector information. The level of sensitivity refers to the degree to which, and the extent or duration of, any impacts to the confidentiality of public sector information.
Significance	An assessment outcome (using the BILs) that considers compromise to the integrity and/or availability of public sector information. The level of significance refers to the degree to which, and the extent or duration of, any impacts to the integrity and / or availability of public sector information.
Significant change	A substantial change to the organisation's operating environment (e.g. new function added/removed impacting on the type of information that the organisation handles, changes to the threat landscape) impacting on the organisation's identified information risks.
Standard(s)	High-level statement describing the key principles of what needs to be achieved. Also refer to the *Victorian Protective Data Security Standards (VPDSS)*
Statement of Applicability	Identify the element(s) that modify risks to public sector information. This is informed by: • the organisation's criteria for risk treatment options; and • the way in which elements interact with one another to provide 'defence in depth'. Where an organisation believes elements do not apply to them, supporting justification should accompany such decisions.
Statement of Objective	A high-level description outlining the intent of the Standard. Also referred to as Objective(s).
Third party	Any external party outside of the organisation. This can include another organisation (public or private), a contracted service provider, or individual.

Unofficial information	Information that is not related to Victorian Government activities, such as a personal email. Labels such as 'Unofficial' or 'Private' are not protective markings. These terms describe content that has been created or received in an individual's private capacity.
Victorian Protective Data Security Framework (VPDSF)	Required under section 85 of the PDPA. This is the overall scheme for the security of Victoria's public sector data. The framework consists of the Victorian Protective Data Security Standards and the monitoring and assurance model to be used to assess the effectiveness, efficiency and economy of security practices across the Victorian public sector.
Victorian Protective Data Security Standards (VPDSS)	Required under section 86 of the PDPA. '*The Commissioner may issue standards, consistent with the Victorian protective data security framework, for the security, confidentiality and integrity of public sector data and access to public sector data (protective data security standards).*' The Standards cover governance and the protective security domains of information, personnel, ICT and physical security.

Term	Expansion
BIL	Business Impact Level
CIA	Confidentiality, Integrity, Availability
DLM	Dissemination Limiting Marker
ICT	Information Communications Technology
IMM	Information Management Marker
ISM	Information Security Manual
ISMF	Information Security Management Framework
FOI	Freedom of Information
OVIC	Office of the Victorian Information Commissioner
PDCA	Plan, Do, Check, Act
PDP Act	Privacy and Data Protection Act 2014
PDSP	Protective Data Security Plan
PSPF	Protective Security Policy Framework
RACI	Responsible, Accountable, Consulted, Informed
SOA	Statement of Applicability
SRPA	Security Risk Profile Assessment
VGRMF	Victorian Government Risk Management Framework
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards
VPS	Victorian Public Sector
WoVG	Whole of Victorian Government