Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards – Glossary

Version 2.1 January 2022

Document Details

Victorian Protective Data Security Standards Glossary	
Protective Marking	N/A
Approved for unlimited public release	*Yes – Authorised for release*
Release Date	January 2022
Review Date	January 2023
Document Version	2.1
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.vic.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
2.1	January 2022	**Added new terms:** • Active • Assurance • Augmented Backus–Naur form • Critical Infrastructure Information • Current (information) • Custodian (information asset) • De-identification • Direct access • Disposal • Document • Email Protective Marking Standard • Entrusted persons • Event (information security) • Incident (information security) • Industrial Automation and Control System • Information sharing arrangement • Information security lead • Non-current (information) • Persons (all) • Privacy • Risk based control analytics • Security clearance **Updated the following terms:** • Agreement • Arrangement • Availability • Business Impact Levels

		• Caveat • Community of Practice • Control(s) • Dissemination Limiting Marker • Functional equivalent • Guides • High assurance roles/functions • Information (asset) owner • Information release • Information security value assessment • Information sharing • Integrity • Legacy information • Personnel security • Primary source • Protective Data Security Plan • Protective marking(s) • Public sector data • Security classification • Security measure • Security value • Victorian Protective Data Security Framework • Victorian Protective Data Security Standards **Removed the following terms:** • Impact level(s) • Value

Term	Definition
Active (information)	See ‘Current’ (information)
Agency	As per *Privacy and Data Protection Act 2014*, 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 of 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, people and/or system-based assets to support that organisation’s business functions, services and activities. Value can be subjective or objective.
Assurance	A degree of confidence that an organisation is managing information security risks, in the context of the VPDSF.
Augmented Backus–Naur form	A system of a language used as a bidirectional communications protocol for emails.

Availability	The desired state that allows authorised persons and/or systems to access defined information for authorised purposes at the time they need to do so.
Body (public sector)	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 of the *Privacy and Data Protection Act 2014* 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 Levels	Scaled impacts describing the harm or damage to government operations, organisations or individuals, resulting from a compromise of the confidentiality, integrity and/or availability of public sector information. Business Impact Levels are used to determine the security value of public sector information.
Caveat	A warning that the information has special requirements in addition to those indicated by an accompanying security classification. Caveats cannot be applied on their own.
Community of Practice	An organised group of people who share common interests, passions, or concerns for something they do, collaborating to resolve issues, improve skills, share knowledge and learn from each other's experiences. Otherwise referred to as a Special Interest Group.
CONFIDENTIAL	A legacy security classification under a superseded protective marking scheme.
Confidentiality	The limiting of public sector information to authorised persons and/or systems 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. Otherwise referred to as outsourced service providers.
Control(s)	Measure that maintains and/or modifies risk. Note: This may include specific policies, procedures, processes and technologies. [SOURCE: ISO 31000:2018, 3.8, modified – Note added]
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, or rendered unavailable for an extended period, or destroyed, would significantly impact on the social or economic wellbeing of the organisation or Victorian community.
Critical Infrastructure Information	Information related to critical infrastructure as defined in the *Emergency Management Act 2013*.
Critical services	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.
Current (information)	Information that is being actively used. Otherwise referred to as '*Active*'.
Custodian (information asset)	A nominated individual and/or group who is formally responsible for day-to-day management of the delegated assets in their care. Custodians direct how the information asset is managed and used on behalf of the owner. Custodians are responsible for ensuring information asset quality is in line with user and business needs and fit for purpose.
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	See 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.
De-identification	The *Privacy and Data Protection Act 2014* defines personal information as de-identified when it no longer relates to an identifiable individual or an individual that can be reasonably identified. De-identification involves removing or altering any data that identifies an individual or is reasonably likely to do so. The context in which the data will be used or disclosed also needs to be considered. In most cases the de-identification process involves removing direct personal identifiers (such as a name, address, or Medicare number), and then removing or altering any remaining indirect or quasi-identifiers (such as date of birth, gender, profession, or rare conditions) that might permit identification when used in combination with auxiliary data or information available elsewhere. Any use or disclosure of de-identified data outside a closed or protected environment carries the risk of re-identification occurring with the use of auxiliary data or information.
Direct access	The ability, right, or permission to collect (obtain), hold, manage, use (interact with or retrieve), disclose or transfer public sector information (data) from information holdings or systems. The viewing of information or information systems that has been released in an authorised manner is not considered direct access.
Dissemination Limiting Marker	A legacy 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.

Disposal	The implementation of appraisal decisions authorised by retention and disposal authorities or other instruments. The secure destruction or deletion of information/records from organisational systems; the migration of information/records between systems; and the transfer of records to PROV and/or to secondary storage (archive).
Document	As defined in section 3 of the *Freedom of Information Act 1982.*
Element(s)	A security measure that modifies risk. Elements often depend on a supportive control environment to be effective. Also referred to as VPDSS Elements.
Email Protective Marking Standard	A standardised format for protective markings (and, where relevant, information management markings) on emails exchanged in and between Australian Government entities.
Entrusted persons	Individuals occupying a role or performing a function where: • it is expected that they will access information, assets, facilities or engage in processes that are placed under some form of control or restriction because of their value (sensitivity and significance); and/or; • a higher level of assurance is required (see definition of high assurance roles/functions).
Event (information security)	Occurrence indicating a possible information security breach or failure of controls. [SOURCE: ISO 27002]
Functional equivalent	Alternative security measure that provides the same or better functionality as the specified control. An exception is not required in this instance.
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 Practitioner guides or security guides.

High assurance roles/functions	Roles or functions that have high levels of privilege and or influence associated with their role (e.g., credit controllers, system administrators, senior executives). These roles or functions may not necessarily have access to security classified information or assets but have the ability to influence important organisational outcomes and management of public sector information.
Incident (information security)	One or multiple related and identified security events that can harm/damage an organisation, its assets, individuals or compromise its operations. Information security incidents may take many forms, such as compromises of electronic information held on government systems and services and include information in physical formats (e.g., printed, photographs, or recorded information either audio or video) and verbal discussions.
Impact statements	The effect, result or outcome of something occurring from a compromise of public sector information. An impact statement describes a natural or logical outcome from an action or condition.
Impact category	Grouping of ‘like’ impacts that are derived from a similar family/topic.

Industrial Automation and Control System	A collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process. NOTE - These systems include, but are not limited to: • industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety-instrumented system (SIS) functions, whether they are physically separate or integrated), • associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems, and • associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes. [SOURCE: IEC/TS 62443-1-1 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models]
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 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 Information Communications Technology 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	A discipline 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	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 (asset) owner	A nominated role or entity accountable for the secure management of all information generated by, or on behalf of them, and/ or under their control.
Information release	Authorised dissemination and/ or disclosure of public sector information. N.B. This is different to the term ‘direct access’ (see direct access definition).
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 sharing arrangement	An arrangement by which an information owner specifies security measures that third parties must implement and maintain to gain access to or a copy of the information. An information sharing arrangement provides a level of assurance around the ongoing security of the information once the material has left the direct control of the information owner.
Information Security Management Framework	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 lead	A central point of contact for OVIC, helping deliver important information security messages and updates relating to the VPDSF and VPDSS. An information security lead can also help coordinate or guide the implementation of the VPDSS on behalf of the organisation. There is no set role that this function should be assigned to but should be someone who has the ability to influence good information security outcomes for the organisation.
Information security value assessment	An assessment process that considers compromise of the confidentiality, integrity, and/or availability of public sector information, to determine its overall security value (highest Business Impact Level).
Information sharing	The authorised exchange of information with a third party on a systematic or ad hoc basis.
Integrity	Assurance that public sector information and/or systems have 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.

National interest	A matter which has, or could have, an impact on Australia, including matters related to: • 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.
Non-current (information)	Information that is not being actively used and has been archived or superseded.
Organisation	The collective term for Victorian public sector organisations, defined as an 'applicable' agency or body under section 84 of the *Privacy and Data Protection Act 2014*.
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.
Persons (all)	Any individual (employees, and any third parties such as contractors, consultants, volunteers, etc.) with direct access to public sector information and/or information systems.
Personnel security	The management of personnel across multiple phases, including: • pre-engagement (eligibility and suitability); • engagement (ongoing and re-engagement); and • separation (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. Physical security includes planning, selection, building, and modification through to disposal of assets and facilities, or retirement of services.
Primary source	Reference point where a VPDSS 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.
Privacy	A human right under the UN Declaration of Human Rights and the *Victorian Charter of Human Rights and Responsibilities Act 2006*. Privacy encompasses several overlapping concepts including the right to be left alone and shielded from the attention of others, secrecy (concealment of information from others), control of personal information, and the protection of one’s personality, individuality and intimate relationships.
Protective data security	See Information Security.
Protective Data Security Plan	As required under section 89 of the *Privacy and Data Protection Act 2014*. A PDSP is a formally endorsed document, used by VPS public sector body Heads to: • advise OVIC of their maturity level, and implementation status of the VPDSS, referencing information security risks as identified as part of the SRPA process; • document the organisation’s security profile; and • attest to the implementation activities as required by the VPDSS.
Protective data security standards	See Victorian Protective Data Security Standards or Standards

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 using the Business Impact Levels. Protective markings inform the minimum level of protection to be provided throughout the information lifecycle (i.e., 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 4 of the *Privacy and Data Protection Act 2014*.
Public sector data	Any information (including personal information) obtained, received, or held by an agency or body to which Part 4 of the *Privacy and Data Protection Act 2014* applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body. This includes structured and unstructured data. Also referred to as public sector information.
Public sector information	See 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 VPDSS. Resources include practitioner guides, information sheets, reference material, templates, working examples, ready reckoners, visuals, etc.
Risk appetite	The type and amount of risk that an agency is prepared to accept or avoid. [SOURCE: Victorian Government Risk Management Framework]

Risk based control analytics	An approach that analyses the appropriateness and effectiveness of existing controls, as well as the prioritisation of planned controls (treatments), to reduce risk to a target level.
Risk posture	An organisation’s overall risk position, that is, current business and strategic risks being managed.
Risk profile	See 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	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. [SOURCE: Victorian Government Risk Management Framework]
Security	The preparedness, protection and preservation of people, property, and information both tangible and intangible (from threat).
Security areas	Refers to key areas or disciplines of information, Information Communications Technology, personnel and physical security N.B. Governance is not traditionally recognised as a core security area but is an essential component of the VPDSS. Also referred to as a *Security Domains.*
Security attributes	Refers to the confidentiality, integrity, and availability requirements of public sector information.
Security by Design	A methodology that enables security to be ‘built in’ to the design and architecture of information systems and business processes. Security by Design 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 classification	Public sector information that has been security assessed as having at least a Business Impact Level of 2 (high) to protect the confidentiality attributes of the information. This results in a security classification as a protective marking. Security classifications include PROTECTED, SECRET and TOP SECRET.
Security clearance	A status granted by the Australian Government Security Vetting Agency or Authorised Body to an individual who has successfully undergone the personnel security vetting process. This process assesses the individual's eligibility and suitability to access security classified information and assets, and/or occupy a role or perform a high assurance function.
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	See control(s).
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	As required under section 89 of the *Privacy and Data Protection Act 2014*. A process that organisations undertake to assess and manage information security risks.
Security value	The highest overall business impact of the public sector information/information systems, based on a holistic assessment of compromise to the confidentiality, integrity and or availability.
Sensitivity	An assessment outcome (using the Business Impact Levels) 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 Business Impact Levels) that considers compromise to the integrity and/or availability of public sector information/information systems. 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/information systems.
Significant change	A substantial change to the organisation’s operating environment impacting on the organisation’s information risks (e.g., a new function added/removed impacting on the type of information that the organisation handles, or changes to the threat landscape).
Standard(s)	High-level statement describing what needs to be achieved by the organisation. Also referred to as the Victorian Protective Data Security Standards or 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 statement of the intent of the Standard, identifying the desired outcome when the Standard has been achieved. Also referred to as Objective(s).
Third party	Any person or entity external to 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	A framework, established under Part 4, section 85 of the *Privacy and Data Protection Act 2014*, developed to monitor and assure the security of public sector information, and information systems, across the VPS. This is the overall scheme for the security of Victoria's public sector data.
Victorian Protective Data Security Standards	Required under Part 4, section 86 of the *Privacy and Data Protection Act 2014*. '*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 areas of information, personnel, Information Communications Technology, and physical security. The Standards offer high-level statements describing what needs to be achieved by the organisation.

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