Data Exchange Standard

Standard

Departments must exchange and share data in accordance with the requirements set out in this standard.

Document Control

Applies to	All departments and Victoria Police	**Authority**	CIO Leadership Group
Period	2019-2021	**Advised by**	Digital Strategy and Transformation, Department of Premier and Cabinet
Issue Date	September 2019	**Document ID**	IM-STD-10
Review Date	September 2021	**Version**	1.0

Except for any logos, emblems, trademarks and contents attributed to other parties, the statements of direction, policies and standards of the Victorian Government's Victorian Secretaries Board or CIO Leadership Group are licensed under the Creative Commons Attribution 4.0 International licence. To view a copy of this licence, visit https://creativecommons.org/licenses/by/4.0/

Requirements

In this standard, ‘exchange’ is synonymous with sharing and refers to the one or two-way transfer of structured data in a secure, authorised and predefined way, whether:

- automated
- real-time or near real-time
- system to system
- via email
- via secure file transfer
- bulk uploads, ongoing or once-off
- any other form of exchange not listed above e.g. USB.

'Structured data' refers to data that can be organised and stored in fixed fields such as in a relational database record or spreadsheet. 'Unstructured data' does not conform neatly into a fixed field format. Examples include data streams, social media data, documents, emails, videos, audio files, and images.

When exchanging data, departments must at a minimum:

Requestor (requesting department)

1. Include in a request for data:
    - The purpose and background context for the data request
    - A clear description of the data required
    - How the data will be used
    - Whether the data will be shared or distributed and to whom
    - Whether the request is once-off or on-going and under what conditions the data will be exchanged and managed.
2. Request data which contains ‘sensitive[1]’ data only where allowed under the relevant authorities listed in requirement 3.

Provider (providing department)

3. Evaluate all data requests to assess whether the department has the right (or authority) to exchange the data requested including:
    - Legislative authority or obligation to share under legislation (Acts) relevant to the department or portfolio.
    - Legislative authority to share under the *Privacy and Data Protection Act 2014* , *Victorian Data Sharing Act 2017*, *Public Records Act 1973* and *Freedom of Information Act 1982*

[1] ‘Sensitive’ data is data with a Business Impact Level (BIL) of Limited or higher or data with a protective marking of Cabinet-in-Confidence (as per the Office of the Victorian Information Commissioner’s (OVIC) guidance on Business Impact Levels and Protective Markings)

- Other regulation and policies specifically relevant to the department or portfolio.
- If the Provider is not the owner of the data, whether there is:
  - a commercial agreement
  - personal individual consent or
  - data asset owner's consent (if the data is owned by another department or agency)

  that permits the exchange of data (noting that permission to exchange may only be for certain limited purposes).

4. Evaluate all data requests to assess whether the department is ready to exchange the data requested including:
   - Carrying out a risk assessment to determine risk to the department, the Victorian Government (government) and the Victorian Public (see the Victorian Government's Risk Management Framework)
   - Ensuring that where 'sensitive' data is involved, that a privacy impact assessment is conducted to ensure reasonable steps have been taken to protect the data from misuse or loss and unauthorised access, modification or disclosure (see the Office of the Victorian Information Commissioner's (OVIC) guidance on Information Sharing and Privacy Impact Assessments)
   - Ensuing data is de-identified wherever possible, unless identified data is essential to enable the data to be fit-for-purpose (see OVIC's guidance on de-identification Protecting unit-record level personal information).
   - Assessing whether the Provider and the Requestor have the appropriate processes, technology and infrastructure in place, and sufficient capabilities and capacity to undertake the exchange
   - Whether the data is of sufficient quality to be fit-for-purpose, and if not, to provide appropriate disclaimers as to its use.
5. Disclose 'sensitive' information only to the extent required to meet the objectives of the request, and only in accordance with the provisions of the authorities listed in requirement 3.
6. Ensure that all data exchanges are accompanied by a data exchange arrangement - legally binding, non-legally binding or Creative Commons licence (see Creative Commons Australia). The type of arrangement used should be based on who the department is exchanging data with, the level of data protection required, and the level of risk associated with the data and the data exchange, see Table 1 in Supporting Information.
7. Ensure all legally binding and non-legally binding data exchange arrangements include the minimum requirements outlined in Table 2 in the Supporting Information.

8. Exchange data to the maximum extent possible under a Creative Commons licence and release via data.vic.gov.au as open data unless restricted for reasons of privacy, public safety, security and law enforcement, public health, and compliance with the law[2].

Legal advice should be sought to ensure that data is exchanged in a way that complies with the department's applicable statutory authority and administrative obligations.

General

9. Record all requests and data sharing arrangements into a register of data exchange initiatives for government probity and transparency and in accordance with the Victorian Protective Data Security Framework and Standards.
10. Ensure data exchange arrangements comply with the requirements for managing public sector data under the Victorian Protective Data Security Framework and Standards.
11. Incorporate data exchange policy and associated processes into department-wide data or information management strategy, policies and processes. Key considerations include data governance and authority, roles and responsibilities, data definitions, data security classifications, risk assessment, data exchange arrangement tools, data transmission methods and issue management.
12. Ensure all data exchanges are authorised by an officer of the organisation at a level commensurate to the risk associated with the data and in accordance with the government's Policies and standards for government IT.
13. Appoint an owner and custodian in each of the Requestor and Provider organisations who will be accountable and responsible for the data exchange.

See the Data Exchange Guideline and associated tools for help in implementing this standard.

Overview

Departments exchange (or want to exchange) data for various purposes and uses. However, factors and variations in legislative, regulatory, policy and contractual requirements, data types and formats, security classifications, processes and protocols, arrangement mechanisms, capabilities, capacities and appetites for risk impact the ability of one organisation to exchange data with another.

Given the variability in methods used, the Data Exchange Framework (framework) provides a common approach to exchanging or sharing data internally and externally to government. This Data

[2] As per Principle 4 of the Information Management Policy and Principle 1 of the DataVic Access Policy Guidelines For The Victorian Public Sector. Refer to this guideline for information on what data should and should not be made available.

Exchange Standard (standard) supports the framework by setting out the minimum requirements to enable data to be exchanged.

This standard refers specifically to structured data, unstructured data are not covered by this standard.

Rationale

The government aims to enable data sharing and integration to support evidence based decision-making, increase the value of its invest in data and better services in a safe and secure environment. This objective is captured through the principles underlying the government's Information Management and DataVic Access Policies which state:

- Principle 4 (Information Management Policy): Information is shared and released to the maximum extent possible
- Principle 1 (DataVic Access Policy): Government data will be made available unless access is restricted for reasons of privacy, public safety, security and law enforcement, public health, and compliance with the law.

The Data Exchange Framework has been developed with these tenets in mind and aims to:

- Enable, encourage and authorise data exchange to increase the value of the investment in government data and ease the sharing and / or integration of data
- Reduce the cost and resource intensity of data exchange
- Maintain data integrity by considering the quality, value and authenticity of the data being exchanged
- Balance the need for safety and transparency in data exchange with the need for better informed decisions, evidence-based policy development, performance reporting and operational efficiency
- Ensure data exchanges are fit-for-purpose (i.e. meet business needs) and able to be supported.

The framework standardises the data exchange approach, regardless of data type, classification, exchange method, platform, or intended use.

Derivation, scope and glossary

Derivation

This standard is derived from the government's Data Exchange Framework and is guided by the Information Technology Strategy Victorian Government 2016–2020 (IT strategy).

Scope

All departments and Victoria Police, referred to collectively as 'departments', are formally in-scope. While not required, the standard may be adopted by agencies and partner organisations, if desired.

Glossary

Unless otherwise stated, the glossary of terms and abbreviations used in this document are defined in the Information Management Glossary.

Related documents, tools and references

- Creative Commons Australia
- Data Exchange Framework
- DataVic Access Policy
- *Freedom of Information Act 1982*
- Freedom of Information Guidelines
- Guidelines for Sharing Personal Information
- Information Management Framework
- Information Management Governance Standard
- Information Management Glossary
- Information Management Policy
- Information Technology Strategy Victorian Government 2016-2020
- Intellectual Property Guidelines for the Victorian Public Sector
- *Privacy Act 1988 (Cth)*
- *Privacy and Data Protection Act 2014*
- *Public Records Act 1973*
- Public Record Office of Victoria (PROV) Standards Framework and Policies
- *Victorian Data Sharing Act 2017*
- Victorian Government Risk Management Framework
- Victorian Protective Data Security Framework (VPDSF)
- Victorian Protective Data Security Standards (VPDSS).

Further information

For further information regarding this standard, please contact Digital Strategy and Transformation, Department of Premier and Cabinet, at: digital.transformation@dpc.vic.gov.au.

Supporting information

Data exchange arrangement

All data exchanges must be accompanied with a documented data arrangement. The type of arrangement (legally binding, non-legally binding or Creative Commons licence) and format of the arrangement (formal or informal) will depend on who the data is being shared with i.e. internal or external to the department, associated risk and level of data protection required.

Table 1: Criteria determining the use of arrangement types

Requestor →	**Internal**	**External**				
		Victorian Government			**Non-Victorian Government**	
	Refers to requestors that are internal to the provider organisation (3)	**Refers to Victorian Government departments and agencies. Note, while statutory bodies are part of the government, they are legal entities in their own right. A legally binding agreement should be entered into with a statutory body when warranted by the associated level of risk**			**Refers to all other entities including government funded entities outside of government, local government, federal government, governments in other jurisdictions and any non-government entities**	
Data risk	All levels (1)	Not sensitive (1)		Sensitive	Not sensitive (1)	Sensitive
Arrangement type	Non-legally binding	Non-legally binding	Legally binding	Non-legally binding	Legally binding	
Format	Informal	Informal	Formal	Formal	Formal	Formal
Example arrangement	Email	Email	Licence such as creative commons (2)	Memorandum or letter of understanding (or other formal non-legally binding mechanism)	Licence such as creative commons (2)	Legal Agreement

(1) If data is not 'sensitive', the Provider should consider releasing it as open data, as per Principle 4 of the Information Management Policy and Principle 1 of the DataVic Access Policy Guidelines For The Victorian Public Sector. Refer to the DataVic Access Policy Guideline for information on what data should and should not be made available.

(2) Refer to Creative Commons Australia (who provide copyright licences to facilitate sharing and reuse of creative content) and DTF's Intellectual Property Guidelines for the Victorian Public Sector for further guidance.

(3) For example, a requestor internal to the organisation Department of Health and Human Services (DHHS) is a person within a branch, division or business unit of DHHS. Other 'bodies' (agencies, statutory bodies, etc.) related to DHHS, such as Family Safety Victoria (FSV) and the Victorian Agency for Health Information (VAHI) are considered external to the organisation of DHHS.

Further guidance is provided on the recommended type and format of arrangement to suit certain circumstances in the Data Exchange Guideline.

Table 2 below describes the minimum requirements for creating the different types of data sharing arrangements (excluding licences such as creative commons, which will have their own terms and conditions). These requirements are additional to standard terms and conditions found in a legal arrangement such as definitions, interpretations, compliance with laws, dispute resolution, variations, breach provisions and termination.

In the case of a formal arrangement (excluding licenses), if more than one dataset is to be exchanged with the same Requestor, it is recommended that general requirements that apply to any data

exchange be captured in the terms of the arrangement and any specific requirements around datasets be captured in the schedules (i.e. each dataset should have its own schedule).

Table 2: Minimum requirements for a data exchange arrangement

Requirement	Description	Arrangement type (Applicability)		
		Non-legally binding		Legally binding
		Informal (e.g. email)	Formal (e.g. MOU, LOU)	Formal (Legal Agreement)
Purpose	The purpose of the initiative that underpins the data exchange, including the associated outputs, benefits and outcomes to be achieved and how the data will be used to achieve these benefits and outcomes.	Yes	Yes	Yes
Background	Context around the initiative and the basis for the data exchange including relevant statutory powers, government policies, operational needs and organisational strategic directives.	Yes	Yes	Yes
Period of agreement	Commencement date of the agreement, how long the agreement will be in place and / or the end date.	Yes	Yes	Yes
Key contacts	Names, roles and contact details of the appointed representatives of each party to the data exchange arrangement.	Yes	Yes	Yes
Obligations	The roles and responsibilities of each party, governance structures in relation to the arrangement and that all appropriate authorisations have been sought. This may include principles around data exchange.	Conditional (1)	Yes	Yes
Data description	Description of the data being exchanged, including data types, timeframes (e.g. data from 2010 – 2018, broken down by month), data-related standards used (e.g. metadata standards, GIS standards, industry standards), data security classification, whether the data has been de-identified and the method used.	Yes	Yes	Yes
Terms of use and disclosure	How the data will be used, joined or integrated, de-identified for privacy[3], reproduced, published internally, externally or not at all, or commercialised. With whom may the Requestor share or distribute the data or outputs resulting from using the data and under what conditions this may occur.	Conditional (1)	Yes	Yes

[3] Refer to the *Privacy and Data Protection Act 2014*.

Requirement	Description	Arrangement type (Applicability)		
		Non-legally binding		Legally binding
		Informal (e.g. email)	Formal (e.g. MOU, LOU)	Formal (Legal Agreement)
Intellectual Property (IP) and licensing	Who has ownership of the data and IP rights? Who will own any new IP developed? Can the Requestor use the data for commercial purposes or building a brand or reputation and under what conditions? This may include a Creative Commons licence and associated attribution.	No	Yes	Yes
Data quality statement	Details of the quality of the data. A data quality statement will be provided in the first instance and updated when there are changes to the any of the seven data quality dimensions, in accordance with the Data Quality Standard.	Conditional (1)	Yes	Yes
Data exchange and management	How the data will be transmitted (methods and standards) by the Provider to the Requestor, how the data will be managed by the Requestor, including data security and privacy[3] (including de-identification). Guidance is provided by the Victorian Protective Data Security Framework and Standard.	Yes	Yes	Yes
Service levels	Service levels around the provision of data including service availability and reliability targets, maintaining data quality (including de-identification of data), complaints handling process and response times and consequences of not meeting service level targets.	Conditional (2)	Conditional (2)	Conditional (2)
Change management	The process for managing changes to the data provided - what, how, who and when this is communicated from the Provider to the Requestor.	No	Conditional (2)	Conditional (2)
Data retention / disposal	Relevant data retention periods and whether the data should be returned to the Provider or disposed of at the end of the retention period.	No	Yes	Yes
Breach in data use or disclosure	Outline the process for managing unauthorised use or disclosure of data and any sanctions for failure to comply.	Conditional (1)	Yes	Yes
Fees or charges	Outline any fees or charges that apply for providing the data and payment terms and conditions. This will apply only in certain circumstances[4].	No	No	Yes
Compliance	The Provider's rights to monitor compliance with the exchange standards and terms of the agreement.	No	No	Yes

[4] Principle 8 of the Intellectual Property Guidelines for the Victorian Public Sector states that an agency (all departments and public bodies) may commercialise, or apply the Cost Recovery Guidelines to intellectual property if:

a) it has an explicit statutory function to do so; or

b) it has been explicitly authorised by the Treasurer to do so because of a clear net benefit to the Victorian community.

Requirement	Description	Arrangement type (Applicability)		
		Non-legally binding		Legally binding
		Informal (e.g. email)	Formal (e.g. MOU, LOU)	Formal (Legal Agreement)
Review of arrangement	If the arrangement is a rolling arrangement, there should be a date to review its ongoing effectiveness.	No	Conditional (2)	Conditional (2)
Schedules to the arrangement	A separate schedule should be provided for each dataset exchanged and should include the dataset name, description, data owner (or custodian), data fields, data definitions, data quality statement and data security classification.	No	Conditional (3)	Conditional (3)

Conditional (1) Applies if personal or sensitive information or confidential data are involved

Conditional (2) Applies if data provision is recurring (i.e. not one-off)

Conditional (3) Applies if more than one dataset is exchanged

Document Control

Approval

This document was approved by the CIO Leadership Group on 16/07/2019 under authority of the Victorian Secretaries Board and applies from the date of issue.

Version history

Version	Date	Comments
0.1	14/05/2019	Version for review by stakeholders
0.2	30/05/2019	Incorporated feedback
1.0	07/06/2017	Final