Data Exchange Technical Specification Template

Introduction

Overview

The Data Exchange Technical Specification Template (template) highlights key technical details that should be documented around a data exchange between a data providing department (Provider) and a requesting department (Requestor). Please refer to the original Data Exchange Request Template and any supporting documentation provided for further information relating to the data exchange and documented data arrangement.

Please refer to the Data Exchange Standard for the minimum requirements in undertaking a data exchange and the Data Exchange Guideline for further information on data exchange technical considerations.

'Department' refers to all Victorian Government departments and Victoria Police.

Document purpose

The purpose of this template is to summarise the technical specifications around a data exchange. The template outlines the key technical characteristics around the data and how it is transmitted and managed.

The document should be updated by either party and communicated to the other party if there are changes to the specifications.

Audience

Participants, especially technical specialists in Information Technology and Information Management involved in the data exchange in the Provider and Requestor organisations.

Instructions for use

1. Use of this template is optional, as parties may prefer to use their own technical specification templates.
2. This document should be completed once a data exchange arrangement has been agreed and the exchange process has been successfully tested.

3. This document should be completed by both the Provider and Requestor (in the relevant sections indicated in the template) in consultation with each organisation's Information Technology and Information Management subject matter experts.

4. As the template is being completed, remove the brackets and instructions e.g. <instructions> throughout the document. Remove the introduction pages upon completion of the template.

The template should be adjusted to suit your specific department and or data exchange needs.

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.

Template Document Control

Applies to	All departments and Victoria Police	**Authority**	CIO Leadership Group
Period	2019-2021	**Advised by**	WOVG Information Management Group
Issue Date	September 2019	**Document ID**	IM-TEMPLATE-03
Review Date	September 2021	**Version**	1.0

Template Approval

This document was approved by the WOVG Information Management Group under authority of CIO Leadership Group on 02/07/2019 and applies from the date of issue.

Template version history

Version	Date	Comments
0.1	15/04/2019	Version for review by stakeholders
0.2	14/05/2019	Incorporated feedback. Final draft.
1.0	07/06/2019	Final

Data Exchange Technical Specifications

Data Specifications

To be completed by the Provider

a. Data set name

<The name of the dataset.>

b. Data structure

<Document the data schema and model (structure of the data, variables, data types, interdependencies, mappings).>

c. Data definitions

<Provide definitions of the data (data dictionary) to aid interpretation and understanding of the data. Provide supporting documentation, if necessary. E.g. in the case of education data, what is the definition of a 'student'? Is this 'students' from public and private education providers or students at primary, secondary and / or tertiary levels?>

d. Metadata standard

<What is the metadata standard used in providing the metadata document?

Metadata standards may differ depending on the subject matter (health, education, environment, etc) of the data being exchanged. Refer to your IT specialists for further guidance on the appropriate metadata standard that should be applied.>

e. Data security classification

<What is the data security classification of the data?

Data must be classified to ensure appropriate security is applied during the exchange. Data should be classified in accordance with the department's security policy or OVIC's guidance around Business Level Impact and Protective Markings.>

f. Data validation

<Is there any validation that needs to be performed on the data during the exchange? Detail how this will occur and when.>

Data exchange process flow

To be completed by the Provider.

a. End-to-end data exchange Flow

<What is the data exchange flow between the Provider and Requestor i.e. what is the process for exchanging data from when the data is collated, transmitted, used and disposed? This may include a swim lane process flow that shows those responsible for each step in the process.

The process flow will need to incorporate processes undertaken by people as well as systems.>

b. Dependencies

<List any technical dependencies for the data exchange to take place.

E.g. this may include access to systems and environments, or systems undertaking a process at certain intervals therefore requiring those processes to be complete before data is exchanged.>

Transmission specifications

To be completed by the Provider

a. Transmission frequency

<Will the data be exchanged once, or will it be recurring? If recurring, how frequently will the exchange occur (real time, near-real time, daily, weekly, monthly or yearly) and when will it occur (date and time)?>

b. Transmission volume

<What is the size or volume of the dataset to be exchanged? If the exchange is recurring, how will the size or volume of data exchanged change over time? Will the dataset be exchanged as a batch or incrementally as it is generated?>

c. Transmission method

<The transmission method that is used, which should be appropriate for:

- The frequency of the exchange
- The size/volume of the data that will be exchanged
- Whether the exchange will be batch or incremental

- The security classification and level of risk of the data. The higher the risk, the more secure the method required.

E.g. data that contains identified information which is not aggregated would be considered to have high disclosure risk and therefore would require a secure method of transfer. Whereas, data that has been de-identified and aggregated would be considered to have lower disclosure risk and could be transmitted via a less secure method.>

d. Transmission format

<The format or language that will be used to transfer the data, such as:

- CSV, comma separated file
- TXT, plain text file
- XML, type of open data format
- JSON, JavaScript Object Notation
- Standard Interchange Format
- Data Interchange Format
- Open Document Format.>

e. Transmission encryption

<If data encryption is required, what encryption method will be used?

Data encryption is a means of translating data into another form using a key. It is used to maintain confidentiality, such that only people or systems with that key can read the data.

Any encryption applied must be done so using an appropriate method. The Australian Government Information Security Manual provides guidance on appropriate encryption methods based on the security classification of the data.>

f. Infrastructure details

<Details of infrastructure e.g. server address, server access details for both Provider and Requestor that will be used for the exchange.>

g. Error handling

<How errors will be handled when the data is being exchanged. Include a process flow if required.>

h. Issues management - contact details

<Enter the contact name and details for person handling issues around the data exchange for both the Provider and Requestor organisations.>

Data management

To be completed by Requestor

a. Responsibility

<Who is the technical person responsible for the environment in which the data will reside? Enter the name of their role and contact information.>

b. Data Storage

<How and where will data be stored once it is received?

This detail may include server names, systems, hosting location and relevant security standards applied to the environment.

Provide details only if this information differs from the infrastructure details in the transmission specification section above.>

c. Data Security

<How will data be secured once it is received? What are the security controls in place to ensure it is protected from unauthorised access, modification and loss?

The data security controls and measures applied by the Requestor should reflect the data security classification applied by the Provider.>

d. Data disposal

<How will the data be disposed of if the Requestor is to only retain it for a limited time?>

Supporting Documentation

<List the supporting documents relevant to the technical specifications described in this document.>

- <Name (and link where possible).>

Disclaimer

This document is provided “as is”, without warranty to the suitability of the data for unspecified use. The burden of assessment of fitness of the data exchanged lies completely upon the Requestor.

Document control

Version history

Version	Date	Comments

Approvals

Provider approval	Name: Position: Signature: Date:
Requestor approval	Name: Position: Signature: Date: