**TEMPLATE ONLY:** The following annexures are templates to assist Data Providers and Data Users formalise the terms of their Data Sharing Arrangement under the Victorian Public Sector Data Sharing Heads of Agreement (Agreement). These annexures comprise of:

1. Annexure 1 – Data Sharing Schedule
2. Annexure 2 – Privacy Impact Assessment
3. Annexure 3 – Data Security Risk Assessment.

Parties are free to replace all or any part of the annexures with the format/content that best suits their circumstances (noting however for the Agreement to work, the Item numbers and headings should **not** be changed for Annexure 1). For example, Parties may have their own templates and approaches to documenting privacy impact assessments and data security risk assessments.

**INSTRUCTIONS:** Font in blue indicates a need for input or is for guidance only and should be deleted in final versions. There are also drop-down options (font in grey) that support quick completion of the annexures. These boxes can be deleted if not relevant.

Once you have finalised the annexures, please:

1. Clearly date and **mark versions as final**
2. Have authorised contact representatives **complete** the signing page for all annexures
3. **Keep a record** of the formal communication exchanging the final data sharing agreement between the Parties (PDF with signed VPS Data Sharing Heads of Agreement and final signed annexure pack)
4. **Provide a copy to Victorian Centre for Data Insights (VCDI) at DPC** so that VCDI can keep a central data sharing agreements register to provide visibility of the data shared, associated terms and conditions, and to continue to improve these template annexures.

If you need any assistance, please contact VCDI at data.insights@dpc.vic.gov.au.

[**Note**: If your data sharing arrangement proposes to use Personal Information or Health Information for the purpose of data integration, consult the VCDI to discuss whether the *Victorian Data Sharing Act 2017* would be of assistance.]

**Annexure 1**

**DATA SHARING SCHEDULE**

**to the Victorian Public Sector (VPS) Data Sharing Heads of Agreement
dated 16 August 2021**

**[INSERT TITLE OF DATA SHARING ARRANGEMENT AND DATE ARRANGEMENT IS SIGNED]**

|  |  |  |
| --- | --- | --- |
| **Data Provider**: | Choose an item. | [Include any further detail here, as required.] |
|  **Data User**:  | Choose an item. | [Include any further detail here, as required.] |
| **Shared Data (cl 9)**: | [Include general description of proposed data to be shared and select type(s) of information to the right. More detail about the data will be included in the Shared Data table below.]  | [ ]  Personal Information (for example, name, address, phone number, DOB)[ ]  Health Information [ ]  Sensitive information(for example, ethnicity, disability status)[ ]  De-identified information[ ]  Aggregate information [If the data to be shared is aggregate, consider publishing as open data on Data.Vic. For advice on how to do this, please see the [DataVic Access Policy](https://www.data.vic.gov.au/datavic-access-policy), and contact the Data Vic team at  datavic@dpc.vic.gov.au for further information.]☐ Other: |
| **Frequency of provision (cl 9)**: | Choose an item. | [Include any further detail here, as required. If there are multiple frequencies, add a column to the Shared Data table and refer to Shared Data table here.] |
|  **Mechanism of  provision (cl 9)**: | Choose an item. | [Include any further detail here, as required.If there are multiple mechanisms of provision, add a column to the Shared Data table and refer to Shared Data table here.] |
|  **Duration (cl 9)**: | Choose an item. | [Include any further detail here, including exact dates covering duration. Ensure a review takes place if ‘Until further notice’ option is selected.] |

|  |  |
| --- | --- |
| 1. **Permitted Purpose** for which data is provided (cl 8)
 | The data sharing is for the purpose of Choose an item., in line with the VPS Data Sharing Policy. [**Note**: The Permitted Purpose(s) must be within the purposes set out in the VPS Data Sharing Policy, namely for ‘policy making, service planning and delivery’.]The Shared Data (set out in the table below) will be used for [insert specific purpose(s) of using data] to [insert objectives and intended outcomes]. This will have the following public benefits: * [outline the public benefits to be delivered].

[**Note**: The Permitted Purpose(s) should be as specific as possible and where there are multiple purposes, each one should be listed.] |
| 1. **Intended output(s)**(cl 10)
 | Data provided will be used to inform and generate [insert description of intended output(s), including analytics, linkage, producing publication/dashboards, reports, or other public release]. The output(s) will [insert description of how output(s) will contribute to the project objectives and intended outcomes]. The output(s) will be distributed to [insert intended audience] through Choose an item. [specify intended channel for distribution]. It Choose an item. proposed that the output(s) will be reviewed prior to distribution. [Insert details if relevant.]The output(s) Choose an item. confidential. [Insert details.] [**Note**: If the Shared Data is not confidential, consider publishing as open data on DataVic. For advice on how to do this, please see the DataVic Access Policy, and contact the Data Vic team at datavic@dpc.vic.gov.au for further information.] |
| 1. **Data provision and** **security** (cl 12)
 | [Outline the **mechanisms** by which the Shared Data is to be provided, held, managed, used, disclosed, or transferred securely, including information about:* the frequency of supply, who will have access to the data (their roles, qualifications etc.), how and where the Shared Data will be accessed and stored
* how the Data User and Data Provider will meet their Victorian Protective Data Security Standards obligations to maintain the confidentiality, integrity, and availability of the Shared Data
* the relevant security controls and risk treatments (based on **Annexure 3**) for the Shared Data
	+ controls should be drawn from the areas of governance, information, personnel, ICT, and physical security
	+ if the Shared Data is to be combined with other datasets, the whole dataset must meet the controls of the data with the highest security value
* any general assurance processes, principles, frameworks and security controls that are in place, for example, the use of the Five Safes Framework, Privacy by Design, Defence in Depth or any standard operating protocols (attach any relevant assessments or documentation)
* specific assurance mechanisms for how the Data Provider will seek assurance that the Data User will manage the Shared Data securely in accordance with agreed security controls.]

[**Note**: The Data User, in consultation with the Data Provider, must conduct and document a data security risk assessment of the Shared Data at **Annexure 3**.] |
| 1. **Information handling** (cls 10 and 12)
 | [Describe the **conditions** under which Shared Data can be collected, held, managed, used, disclosed or transferred.] [**Note**: Where the Shared Data includes Personal Information or Health Information and as per clauses 8 and 12, this data can only be shared in accordance with Privacy Law. Any relevant exemptions under such laws as well as any privacy risks and how they will be managed must be documented in the Privacy Impact Assessment at **Annexure 2**. Refer to the specific Information Privacy Principle (IPP) in the *Privacy and Data Protection Act 2014* or Health Privacy Principle (HPP) in the *Health Records Act 2001* that gives permission to use and handle the information here. Any terms of use or conditions agreed should also be inserted in this Item. This includes a compliance framework to ensure that controls agreed have been complied with (see Item 10 below).Where the Shared Data contains any confidential information that has restrictions or prohibitions on disclosure (including secrecy provisions), describe how that information will be handled.] |
| 1. **Data quality issues** (cl 9)
 | [Describe any data quality issues, including the obligations of the:* Data Provider to conduct certain checks or take other steps before providing the Shared Data
* Data User to conduct any checks or take other steps before they interrogate and interpret the Shared Data.]
 |
| 1. **On-sharing** **/ requests for data** (cl 10)
 | [Describe how the Data User should handle any requests for Shared Data from third parties and describe the circumstances (if any) in which on-sharing may be permitted (including if the information is Health Information or Personal Information, by reference to Privacy Law), in addition to clause 10. Insert any restrictions around on-sharing, including for example whether the third party should be subject to the same confidentiality requirements as the Data User, or that the third party must comply with Privacy Law.]  |
| 1. **Intellectual property rights** (cl 11)
 | [Describe how the Parties would like to handle Intellectual Property Rights, in addition to or amending clause 11. For example, the Parties may instead wish to agree that if a Data User creates any Intellectual Property Rights using Shared Data provided by the Data Provider, the Data User will grant the Data Provider broader rights than what is contemplated under clause 11.]  |
| 1. **Retention** / **destruction** (cl 13)
 | Subject to any relevant public record keeping obligations that may apply, when the Parties agree that the deliverables have been met and the use of the Shared Data for the Permitted Purpose is no longer required, the Data User agrees to securely [specify period the Data User will retain the Shared Data considering practical needs (for example, to verify output(s) or respond to queries) as well as legal requirements on both the Data Provider and Data User], after which the Shared Data will be securely destroyed via [specify means of destruction in accordance with the security risk assessment]. [Consider also specifying any assurance mechanism required by the Data Provider to certify destruction.] |
| 1. **Authorised contact** **representatives** (cl 14)
 | Data Provider: Choose an item.[Insert name, role, and contact details] Data User: Choose an item.[Insert name, role, and contact details][**Note:** The Authorised contact representatives must have authority to sign the annexures on behalf of their organisations.] |
| 1. **Assurance and other matters**
 | [Include any assurance processes or other matters relevant to this Data Sharing Arrangement not otherwise addressed in this Schedule. For example, *‘Parties agree to an XYZ assurance or audit process to check compliance with agreed controls and risk treatments’*, especially if the Shared Data includes Personal Information or Health Information.] |
| 1. **Termination** (cl 9)
 | [Describe when the Parties may wish to terminate the Data Sharing Arrangement (if any). For example, *‘either Party to terminate by giving X days written notice to the other Party for any reason or for a specified reason, or to terminate without notice in the event of illegal behaviour or if there has been a serious breach of this agreement and the breach cannot or has not been rectified’*.] |

**Annexure 1**

**SHARED DATA TABLE**

[**Notes:**

* The following table is a **template only** with prompts/suggested fields to accurately specify the data intended to be shared. For example, if there are multiple Data Providers and Data Users, you may wish to add columns that specify the relevant Data Provider and Data User pertaining to each dataset or have separate Shared Data Tables. Please replace this table with another if it does not suit your data sharing arrangement’s circumstances.
* The Data Provider should provide all relevant contextual information, including metadata with a clear explanation of data quality, limitations, interpretability, and relevance to ensure Shared Data is used appropriately for the Permitted Purpose.]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Type of Data Requested** | **Data Provider** | **Data Source** | **Need for data in project** | **Variables (if applicable)** | **Level of aggregation(if applicable)** | **Data sensitivities to note(if any)** |
| Insert row number | Name / description of each source dataset required  | Name, Position, Agency/Division of Data Provider responsible for each dataset | Name and system / database where data is located | Describe how this specific dataset contributes to project objectives and Permitted Purpose detailed above | Describe the types of variables requested, for example, demographic, geographic coverage, or any other variable of interest | Select or insert level of detail required  | Highlight key sensitivities or any other special handling requirements for the Shared Data.If the Shared Data contains Personal Information or Health information, briefly note the relevant exemption relied on and refer to **Annexure 2**. |
|  |  |  |  |  | Demographic coverage: Choose an item.Geographic coverage: Choose an item. | Choose an item. | Overall security value: Choose an item.For guidance on assessing the security value of public sector information, see [OVIC’s Practitioner Guide: Assessing the Security Value of Public Sector Information](https://ovic.vic.gov.au/resource/practitioner-guide-assessing-the-security-value-of-information-v2-0/).Protective markings: Choose an item.Information Management Markers [if applicable, otherwise delete]: Choose an item. |

**INSTRUCTIONS:** Once all annexures have been finalised, insert the following signing page at the end of the Annexure pack.

**These annexures, together with the VPS Data Sharing Heads of Agreement dated 16 August 2021, represent the agreement between the Parties.**

|  |  |  |
| --- | --- | --- |
| **SIGNED** by [insert name of authorised contact representative of Data Provider] on behalf of Choose an item.  | )))))))))) |  [Insert role]Choose an item. [Select organisation]Date: ……………………………………………………………. |

|  |  |  |
| --- | --- | --- |
| **SIGNED** by [insert name of authorised contact representative of Data User] on behalf of Choose an item. | )))))))))) |  [Insert role]Choose an item. [Select organisation]Date: ……………………………………………………………. |

**INSTRUCTIONS:** Where Shared Data involves Personal Information or Health Information, the Data User is to complete a Privacy Impact Assessment (PIA), in consultation with the Data Provider.

Insert completed PIA, as part of the Agreement between the Parties. If no Personal Information or Health Information is involved, note this under **Annexure 2** by including words to the following effect: *‘As no Personal Information or Health Information is involved in the Shared Data, there is no need to complete a privacy impact assessment.’*

**Annexure 2**

**PRIVACY IMPACT ASSESSMENT**

**to the Victorian Public Sector Data Sharing Heads of Agreement
dated 16 August 2021**

**[INSERT TITLE OF DATA SHARING ARRANGEMENT AND DATE ARRANGEMENT IS SIGNED]**

[VCDI recommends using the [Office of the Victorian Information Commissioner’s (OVIC) PIA template](https://vicgov.sharepoint.com/sites/DPC-VCDI/Shared%20Documents/Data%20Sharing/07%20Victoria-Victoria%20Data%20Sharing/VPS%20Data%20Sharing%20Framework/Revised%20annexures/ovic.vic.gov.au/privacy/privacy-impact-assessment/).

For assistance on developing a PIA for your project, see OVIC’s guidance on privacy:

[Information Sharing Guide](http://ovic.vic.gov.au/privacy/for-agencies/information-sharing-and-privacy/)

[Privacy Impact Assessments guidance](https://ovic.vic.gov.au/privacy/for-agencies/privacy-impact-assessments/)

[Information Privacy Principles Guidelines](https://ovic.vic.gov.au/privacy/guidelines-to-the-information-privacy-principles/).

[**Note:** All risk treatments identified in this **Annexure 2** should be specified in Item 4 in **Annexure 1**.]

**INSTRUCTIONS:** To mitigate against potential threats that could compromise the security of the Shared Data, the Data User is to complete a Data Security Risk Assessment, in consultation with the Data Provider.

The suggested template below supports the assessment of data security risks. If available, the Parties should use and attach their existing risk management framework and data security risk assessment instead.

This section should ensure that ‘shared risks’ are considered given the context of the Data Sharing Arrangement. Refer to [Victorian Managed Insurance Authority guidance on Managing Shared Risk](https://www.vmia.vic.gov.au/tools-and-insights/practical-guidance-for-managing-risk/managing-shared-risk) for further information and for guidance on risk management.

See the following resources for guidance on this Annexure:

[OVIC’s Practitioner Guide: Assessing the Security Value of Public Sector Information V2.0](https://ovic.vic.gov.au/data-protection/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/)

[OVIC’s Victorian Protective Data Security Standards Implementation Guidance](https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-standards-implementation-guidance/)

[OVIC’s](https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/) *[Practitioner Guide: Information Security Risk Management](https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/)*

[VMIA’s Practical Guidance for managing risk: Identifying, analysing, and evaluating risks](https://www.vmia.vic.gov.au/tools-and-insights/practical-guidance-for-managing-risk/identifying-analysing-evaluating-risks?search-url=/tools-and-insights/practical-guidance-for-managing-risk).

**Note:** All risk treatments identified in this **Annexure 3** should be specified in Item 3 in **Annexure 1**.

**Annexure 3**

**DATA SECURITY RISK ASSESSMENT**

**to Victorian Public Sector Data Sharing Heads of Agreement,**

**dated 16 August 2021**

**[INSERT TITLE OF DATA SHARING ARRANGEMENT AND DATE ARRANGEMENT IS SIGNED]**

**Purpose of this document**

This Data Security Risk Assessment assesses the security risk level and commensurate security risk treatments to support the provision of the Shared Data from the Data Provider Choose an item. to the Data User Choose an item..

**Business Impact Level Assessment and Protective Marking**

[Insert or attach the Business Impact Level assessment here. For guidance on preparing an assessment, see [OVIC’s Practitioner Guide: Assessing the Security Value of Public Sector Information](https://ovic.vic.gov.au/resource/practitioner-guide-assessing-the-security-value-of-information-v2-0/).]

The Business Impact Level for this data has been assessed as Choose an item..

The data is to be marked Choose an item.

**Data security risk assessment**

[This data security risk assessment should consider the context provided in **Annexure 1**.]

The table below details the data security risks that were considered, and the risk rating outcome for providing the Shared Data to the Data User in terms of the likelihood and impact, considering the current security controls. The Data Provider as the risk owner must be able to accept any residual risk and may consider requiring additional risk treatments as part of this arrangement to ensure risks are adequately mitigated.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Riskref.** | **Data security risk** | **Current controls** | **Risk likelihood** | **Risk impact** | **Risk rating** |
|  | Insert identified data security risks using the format of “**Risk of** [insert risk], **caused by** [insert cause], **resulting in** [insert potential impact]”.  | Consider existing controls across the areas of: * physical security
* personnel security
* information security
* ICT security
* Governance.
 | Insert risk likelihood using the drop-down lists below. | Insert risk impact using the drop-down lists below. | Insert overall risk rating based on the Data Security Assessment matrix and using the drop-down lists below. |
| 1. |  |  | Choose an item. | Choose an item. | Choose an item. |
| 2. |  |  | Choose an item. | Choose an item. | Choose an item. |

**Risk treatment plan** [**Note:** Complete this section if there are additional risk treatments required.]

The following table allocates ownership of agreed risk treatments to parties for implementation.

|  |  |  |
| --- | --- | --- |
| **Risk treatment** | **Implementation details** | **Responsible party** |
| Include all risk treatments identified in the Data Security Risk Assessment above.A summary of additional risk treatments should be included in **Annexure 1**, as appropriate. | Include details as to when the treatment is to be implemented, for example, once of prior to sharing, ongoing, etc. | Allocate party responsible for implementing risk treatment. |
|  |  | Choose an item. |
|  |  | Choose an item. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Riskref.** | **Residual risk likelihood** | **Residual risk impact** | **Residual risk rating** |
|  | Insert residual risk likelihood using the drop-down lists below. | Insert residual risk impact using the drop-down lists below. | Insert the residual risk rating based on the Data Security Assessment matrix and using the drop-down lists below. |
| 1. | Choose an item. | Choose an item. | Choose an item. |
| 2. | Choose an item. | Choose an item. | Choose an item. |

**Outcome of risk assessment**

In light of the Shared Data and context of the Data User’s environment, it is assessed that the current security controls and risk treatments Choose an item. mitigate the likelihood and impacts of the key security risks identified.

[**Note:** By signing the signature page to all Annexures, the Data Provider accepts the risk(s) detailed in the Data Security Risk Assessment and all Parties agree to action risk treatments allocated to them in the Risk Treatment Plan.]

***Reference material: Data Security Risk Assessment Matrix***

The following matrix can be used to assess the information security risks with the provision of Shared Data to the Data User. A data security risk assessment should consider the information security value of the information, event likelihood, and the current controls/ mitigating factors that might reduce event likelihood.

|  |  |
| --- | --- |
| **Data security risk assessment matrix** | **Risk impact** |
| **0 – N/A** | **1 – Minor** | **2 – Limited** | **3 – Major** | **4 – Serious** | **5 – Exceptional** |
| **Risk likelihood** | **5 – Almost certain** | Low | Moderate | High | High | Extreme | Extreme |
| **4 – Likely** | Low | Moderate | Moderate | High | High | Extreme |
| **3 – Possible** | Low | Low | Moderate | Moderate | High | High |
| **2 – Unlikely** | Negligible | Low | Low | Moderate | Moderate | Moderate |
| **1 – Rare or N/A** | Negligible | Negligible | Low | Low | Moderate | Moderate |

[**Note:** This matrix aligns with the [Victorian Protective Data Security Framework](https://ovic.vic.gov.au/data-protection/framework-vpdsf/) and [Business Impact Level Table V2.1](https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-framework-business-impact-level-table-v2-1/). Where available, Parties should use their own risk criteria and contextualised Business Impact Level table instead.]