Australian Government
Office of the National Data Commissioner

ONDC

OFFICIAL

Evidence Guidance for Accredited Data Service Provider applications

Contents

Introduction

The Data Availability and Transparency Act 2022 (the Act) commenced on 1 April 2022, establishing a new, best practice scheme for sharing Australian Government data. The ONDC website Resources page provides information on the Act.

The Evidence Guidance for Accredited Data Service Provider (ADSP)applications (Evidence Guide) should be used in conjunction with the:

- ADSP Application Form; and
- Instructions for making an ADSP application.

The purpose of the Evidence Guide is to guide organisations when preparing evidence to demonstrate they meet the criteria for accreditation as a data service provider.

Organisations are encouraged to contact the ONDC for clarification on the process of accreditation in advance of submitting their application.

Preparing evidence for accreditation

Evidence to support an application will be provided under multiple sections in the ADSP Application Form. These are:

- About your Organisation and Data Services
- Data Management and Data Governance
- Privacy and Data protection
- Security Settings
- Skills and Capability
- Consent and declaration.

The following guidance is general and applies to all sections and questions. Specific evidence guidance for each question in the ADSP Application Form is in the next section of this Evidence Guide.

Organisations eligible to apply

Only organisations which meet the definition of 'Australian entity' set out in the Act can be accredited. An Australian entity is: a Commonwealth body, State body or Territory body; the Commonwealth, a State or a Territory; and Australian universities.

An Australian university must be registered in the Australian University provider category, under the Tertiary Education Quality and Standards Agency Act 2011 (Cth) and be established by or under a law of the Commonwealth, a State or a Territory.

Approach to answering the questions

All questions in the ADSP Application Form are required to be answered.

The questions are expressed in broad terms to allow applicants the flexibility in how their evidence is presented, in accordance with the data services the organisation provides and the type of evidence provided.

Accreditation occurs at the organisation level. A condition may be placed on your organisation's accreditation to limit the provision of data services to that part of your organisation providing data services.

While broad organisation level evidence can be provided, the ADSP assessment process will focus on the part of your organisation providing data services and any interlinkages it has with the whole organisation.

For example, evidence for a question relating to staff recruitment arrangements may include corporate level details if these are directly relevant to the part of your organisation providing data services. Another example is for a question relating to staff data skills you may provide evidence that is limited to only those staff in the part of your organisation providing data services.

Evidence for data services

There are three data services an ADSP may provide under the DATA Scheme:

- complex data integration
- de-identification
- secure access

Section 1 of the ADSP Application Form includes questions about which data services your organisation is seeking to provide.

Organisations with limited experience handling Commonwealth data

In this situation, organisations may include evidence:

- drawn from their current data service activities that demonstrates capability against the ADSP criterion; and
- of actions undertaken to implement elements of the criteria that may not previously have been in place demonstrating how the organisation has taken steps to meet the criteria.

The accrediting authority may grant an organisation accreditation with conditions imposed. Conditions could mean an organisation must, or must not, do certain things. A condition of your accreditation may require an organisation to provide, at a specified time, evidence of specified matters to the accrediting authority. Organisations with limited experience handling Commonwealth data may be accredited with conditions imposed as a safeguard to facilitate participation in the DATA Scheme, whilst also supporting these organisations uplift capability over time.

Document standards and classification

To assist with processing, application documents should be in their original format and indicate their currency, any endorsement or approval and any review date.

Organisations may use documentation prepared for other purposes, such as independent audit and can provide documents available on your organisation's public website by weblink.

Documents applicable to multiple questions can be referenced in subsequent questions and are not expected to be duplicated in the application document pack.

Documents up to :Sensitive may be submitted with an application.

Commercial or sensitive details contained in a document may be redacted, however should not be redacted in a way to make them misleading or incomplete for the purposes of assisting to assess appropriateness for accreditation.

Guidance for the application form questions

Organisations are encouraged to contact the ONDC Accreditation team for clarification on evidence requirements for the application form questions. We recommend contact us in advance of submitting the application.

1. About your Organisation and Data Services

Questions in this section provide contextual information about your organisation and data services under the DATA Scheme.

Before completing an application, your organisation should consider its eligibility for accreditation. To be eligible to apply for accreditation an entity must be an ‘Australian entity’ and not an ‘excluded entity’ as defined under the Act. Please contact ONDC if you have any queries regarding eligibility.

Explanation of questions

1.1 Organisation name and email/s for general enquiries.

This question relates to the entity that intends be accredited i.e. a Commonwealth body, State body or Territory body or an Australian University.

The required details are organisation name, legal name of organisation, ABN/ACN, type of entity, and contact email.

1.2 ADSP application co-ordinator (contact officer).

This is the person the ONDC will contact if we have any questions about the application, or if we require further information. Given the volume of documents required for an application, we prefer applicants nominate a co-ordinator in addition to the authorised officer.

1.3 Provide a detailed description of your organisation’s data services under the DATA Scheme.

For the data services that you intend to provide under the DATA Scheme, include the name of the area/sub-unit providing the services. This will make it clear to the assessor which area of your organisation they should focus on when undertaking the assessment.

Your accreditation may include a condition which limits the provision of these services under a data sharing project to those areas and will appear on a public register of ADSPs.

The response to this question should fully describe the data services your organisation provides. You should include:

- comprehensive details of the data services your organisation could provide under the DATA Scheme, including for the area / sub-unit providing data services, a description of each data service, and any specialised services or sectors of expertise such as health, population, housing, environment, etc.;
- who your customers are expected to be; and
- how the data services will be funded.

Customers refers to potential users of your data services under the DATA Scheme, including clients, researchers and analysts.

1.4 Tell us about your organisation’s legal structure, including details relevant to your data services. For example:

- **whether your organisation constitutes a separate legal entity**
- **whether your data services will be provided by an area within the legal entity**
- **if a government body, identify the Group or Division providing the services.**

We seek to understand if your organisation depends on another organisation or a specific area in your organisation to provide data services.

This information assists in understanding the context of data risk for your organisation's data services. For example, dependencies that may affect delivery of data services or operationalisation of data management and data governance frameworks.

Your response may utilise a corporate plan, organisation chart or annual report(s) in explaining your organisation's legal structure and relationship with related and dependent entities and the area providing data services.

1.5 Outline any conflicts of interest (perceived, real or potential) your organisation has, related to providing data services under the DATA Scheme, including contractual commitments.

We require applicants to provide full disclosure of any conflicts of interest or contractual commitments that might impact on your ability to appropriately provide data services.

For any identified conflicts, please explain how these are addressed.

You may include your organisation chart, audit reports, budget reports and/or details of instances where a separation of function was applied in your organisation when handling data.

In response to this question you should include:

- a description of the relevant contractual commitments; and
- demonstration of the separation of functions, such as the separation of research, data analytics or data users from security and system compliance functions.

1.6 Does your organisation have any obligations or affiliations that could impact or conflict with obligations under the Act should your organisation become accredited? Outline these obligations or affiliations and how you will manage these matters.

When you are accredited to participate in the DATA Scheme your organisation will have obligations to keep data safe from unauthorised access. We require disclosure of any obligations or affiliations that might impact on your organisation's ability to appropriately provide data services and safely handle data under the DATA Scheme.

For any identified obligations or affiliations, provide relevant documents and an explanation of how your organisation will manage these matters and obligations to ensure compliance with the Act.

In answering this question you should consider:

- any instance where data or data outputs must be shared beyond participants named in data sharing agreements, including through reporting to parent companies or governance committees;
- any standard contracts or financial arrangements that (will) relate to the future data projects or outputs;
- any members of your organisation based outside of Australia and any standard access they may have to data and data projects; and
- any other relevant foreign influences.

1.7 Are there any legislated functions or restrictions or protections that are specific to how your organisation will undertake data activities?

We need to know of the relevant laws that govern or apply to your organisation's data activities. These may be unique to your organisation and provide context when assessing your application.

Examples may be legislation:

- regarding the functions of your organisation;
- enabling data activities such as collection of data or scope of activity; or
- protections that apply to your organisation's use of data, including any international law obligations.

2. Data Management and Data Governance

The following questions relate to an organisation's ability to ensure the appropriate data management and data governance policies and practices are in place.

Responses should focus on the policies and practices of the area providing data services, including reference to any relevant policies and practices of the organisation.

Where a question response requires corporate level details, this is stated in the guidance for the question.

Explanation of questions

2.1 What data governance policies and practices does your organisation have in place? How do these policies align to the data services your organisation would provide under the DATA Scheme?

This question seeks to ensure data governance policies, processes and procedures are in place to support the organisation operating under the DATA Scheme.

Provide documents (examples below) that describe your organisation's data management and data governance:

- data governance policy, manual or guide;
- data governance program;
- data governance framework; and/or
- data governance chart, process flow or equivalent document.

2.2 What data governance bodies/groups exist in your organisation?

This question seeks to ensure that bodies/groups are in place to oversee the governance of data within the organisation, and to understand the relationships between these groups. Include details explaining the following (or attach relevant documents):

- Terms of Reference for the named bodies;
- membership of relevant bodies;
- the level(s) of seniority of the members of these bodies;
- agendas, minutes or reports from relevant bodies;
- timetable or details of frequency of meetings; and
- how these bodies relate to each other and to other, more general, organisational governance bodies, including reporting lines.
- how issues are escalated within the described governance body structure
- what role these bodies have in developing, implementing, and monitoring the governance policies identified at Q 2.3.

The alignment of corporate level organisation data governance to the area providing data services may be demonstrated by illustrating the governance connection of the data service area to the organisation's data governance framework.

2.3 Tell us about the corporate roles in your organisation that have responsibility for data governance and implementing data policies and practices. Who is the person responsible for data management and data governance within the organisation? Who is the person responsible for data governance within the area providing data services?

This question seeks to ensure data governance roles, responsibilities and accountabilities have been clearly documented, allocated and understood within the organisation.

Identify the data management and data governance roles and accountabilities in your organisation and provide:

- duty, role or responsibility statements of key data governance positions; and
- for the person/s chiefly responsible for data management and data governance provide their role title, name and a brief summary of the qualifications, skills and experience.

2.4 What is your organisation's approach to risk management, and how are data issues monitored and managed under that approach?

This question seeks to ensure that data related risks are effectively managed in relation to the data services provided and endorsed by senior management and continuously monitored.

Provide documents demonstrating risk management of data in your organisation. For example:

- enterprise risk management framework;
- duty, role or responsibility statements of key data risk management roles; and
- risk management committee Terms of Reference and/or membership.

2.5 What audit and review processes does your organisation have in place (internal and external) relating to current and on-going management of data?

This question seeks to ensure data policies, practices and systems are assured and updated through internal and external audit and review programs.

Provide documents demonstrating assurance activities in your organisation. For example:

- audit and review policy, processes, framework or similar documents;
- audit and review workplans; and/or
- copies of reports from recent data audits and/or reviews.

The focus of this question is to demonstrate that your organisation's audit activities, prior audits undertaken and/or future audit plans include coverage of data policies, practices and systems.

The response to this question does NOT require the applicant to initiate an audit.

2.6 Tell us how your organisation will demonstrate public transparency of your data activities and operations, including transparency of processes for data access, confidentialisation, publication or release of data.

This question seeks to understand the public transparency of your organisation's data services and in step with the objectives and requirements of the Act.

In your response, provide:

- data dissemination, publication or release framework, strategy, policy or similar documents;
- links to any relevant supporting documents publicly available; and/or
- public trust framework, strategy, policy or similar document.

2.7 What are the communication channels your organisation has in place, for the lodgement of complaints or stakeholder contact?

This question seeks to ensure your organisation has mechanisms for the public, including data subjects, users and organisations to lodge complaints, trigger investigations and provide feedback.

Provide description and/or documents to show:

- links to publicly available contact information;
- internal complaints and feedback management policies, processes or similar documents; and
- internal and external investigations policies, processes or similar documents.

3. Privacy and Data Protection

The following questions relate to an organisation's ability to ensure privacy, protection and appropriate use of data, and to manage risks.

Responses should focus on the policies and practices of the sub-unit providing the data services and if relevant refer to policies and practices of the organisation.

Explanation of questions

3.1 Tell us about the privacy obligations that apply to your organisation.
How will your organisation apply these privacy obligations under the DATA Scheme, including but not limited to any of the following that may apply:

- **the Commonwealth Privacy Act 1988;**
- **State or Territory privacy laws; and**
- **circumstances where you may have the Australian Privacy Principles (APP)-equivalence term in a data sharing agreement.**

This question is to identify the privacy obligations that apply to the area providing data services and how the area will align these obligations to the privacy coverage condition under the Act.

List the privacy obligations that apply to the area providing data services, including legislation, instructions, codes, national statements on the conduct of research, etc.

Provide an explanation of how privacy obligations would apply under the DATA Scheme, such as the Commonwealth Privacy Act 1988 or law/s of your State or Territory, sector standards and codes.

3.2 Outline your organisation's privacy policy, privacy risk management plan and supporting policies and practices, including:

- **privacy governance processes;**
- **breach and complaints processes; and**
- **how privacy risks are mitigated.**

How will these policies and practices apply to the data services you intend to provide?

This question seeks assurance that organisations providing data services involving personal information have a privacy policy and data management plan, with supporting policy and practices in place for data protection.

Provide documents, as relevant to your organisation that demonstrate your organisation's:

- privacy policies, frameworks or similar documents;
- consent approach, processes, policies, frameworks or similar documents relevant to privacy risk;
- use of Privacy Impact Assessments or similar review process, and copies of relevant reports where available; and
- use of Public Interest Certificates, Public Interest Disclosure or similar processes, and copies of relevant reports, where available.

Responses may include reference to instances of data breach/s occurring and how the organisation handled the matter.

The question response should include explanation of how the organisation's corporate policies and frameworks apply to the area providing data services.

3.3 Tell us about the roles within your organisation that have responsibility over privacy obligations and practices.
Who is the person chiefly responsible in your organisation?
Who is the person chiefly responsible in the area providing data services?

This question seeks to ensure privacy roles, responsibilities and accountabilities have been clearly documented, allocated and understood within your organisation.

Provide documents for the following:

- duty, role or responsibility statements of key privacy positions;
- for the person/s chiefly responsible, provide a brief summary of the qualifications, skills and experience of the person chiefly responsible;
- organisation privacy responsibilities chart, process flow or equivalent document; and
- membership of or participation in relevant professional groups or forums.

As an example, your organisation may have one or more of the following: Privacy Officer, Data Protection Officer, Chief Privacy Officer, and Privacy Champion.

3.4 What policies and practices does your organisation use to ensure its data activities are ethical? Please provide details where your organisation uses ethics committees.

Provide details of your organisation's:

- policies and practices in place that demonstrate ethical data practices, such as data ethics policy; and/or
- documents and processes relating to Human Research Ethics Committee (HREC) approvals or their equivalent.

These organisation documents should be relevant to the data services being provided.

3.5 Tell us about how your organisation ensures that personnel are aware of their privacy and data protection responsibilities and consequences of non-compliance.

This question is looking to ensure staff are aware of their privacy and data protection responsibilities and obligations. The focus is on privacy culture in the organisation.

Provide documents demonstrating the following:

- privacy or related training for staff, including induction and refresher training, frequency and how training records are kept, audited and updated.
- programs and activities to maintain staff awareness and vigilance related to privacy. For example, notices, emails, newsletters, computer lock screens, security patrols, internal communication campaigns, Privacy Awareness Week, etc.
- privacy or confidentiality agreements, declarations, deeds or undertakings signed by staff and how these are stored, audited and updated.

3.6 Tell us about how your organisation ensures personnel involved in providing data services are made aware of their responsibilities handling sensitive information, including personal information.

How are these responsibilities reflected in the culture of your organisation?

This question focuses on how you ensure responsibilities and obligations are implemented when handling sensitive information, including personal information, in the context of the data services your organisation intends to provide.

In your response, provide evidence of procedures that ensure staff involved in providing data services are aware of their responsibilities when handling sensitive information.

Sensitive information shared under the Scheme may be personal information, or other sensitive information e.g. environmental data for protected species.

3.7 Tell us about how your organisation manages customer use of de-identified information and ensures all customers of data services are:

- **aware of their responsibilities when accessing or handling information; and**
- **managed and monitored when accessing information.**

Include your policy, procedures and/or examples of information for customer use.

This question focuses on how your organisation will ensure privacy and data protection responsibilities and obligations are implemented when providing data services.

Customers in this question refers to users of your data services under the DATA Scheme, including clients, researchers and analysts.

Demonstrate how your organisation can ensure customers are aware of their responsibilities. Examples may include:

- undertakings that customers are required to complete;
- training resources;
- how customers are made aware of both what they can and what they cannot do with data they have access to; and
- consistency of customer communication with organisation values.

4. Security Settings

The following questions relate to your organisation's ability to demonstrate effective security measures. The questions are framed to obtain evidence of the security framework and policies and practices that minimise the risk of unauthorised access or sharing or loss of data.

The evidence sought is to provide assurance of the organisation's ability, in the context of providing data services under the DATA Scheme, to:

- identify and manage security risks;
- implement security controls to reduce security risks;
- detect and understand security events to identify security incidents including cyber; and
- respond to and recover from cyber security incidents.

General guidance for Criterion 3: Security Settings

The first question identifies the security framework that your organisation uses to ensure effective security measures are place for all aspects related to the data services to be provided.

The most common frameworks are listed in question 4.1. The subsequent questions for this Criterion:

- detail the minimum requirements for assurance of security measures; and
- focus on the security settings and measures as they apply to the area providing data services.

Where assurance of an independent assessment, against a security framework includes assurance relevant to a question, a description of the assessment will be sufficient evidence. This description should include the recency of the assessment and whether mitigation actions have been undertaken.

Alternatively, if the assessment of the security framework does NOT include the required evidence for a question, the question must be answered in detail.

Explanation of questions

4.1 Tell us about the security framework/s your organisation has been assessed against, and indicate:

- **when the last assessment was undertaken; and**
- **the scope of the assessment, for example a secure access unit or systems used for complex data integration.**

This question captures recent security assessments and reviews undertaken. The evidence should provide details of the:

- scope of the assessment/s and overall findings or ratings;
- high level details of the responses to findings; and
- forward plan for next assessment.

Evidence submitted in your application should NOT include protected or sensitive information about your organisation. Redacted documents will be accepted provided their evidence value to satisfy the question is retained.

The following is an indicative list of security frameworks that may be used as evidence:

- Information Security Registered Assessor Program Assessment (IRAP)
- Information Security Management System (ISMS)/Organisational Protective Security Framework
- Essential Eight Maturity Assessment
- Protective Security Policy Framework
- Australian Competition and Consumer Commissioner Consumer Data Right Accreditation
- ISO27001 Information Security Management (ISMS)
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organisations: A System Life Cycle Approach for Security and Privacy

Organisations using the Essential Eight framework should ideally be aiming for minimum of Maturity Level 2.

4.2 Tell us where your organisation's personnel are located and provide evidence that your DATA Scheme services will be performed or operated only within Australia.
If any part of your data services will be hosted by another organisation or another unit in your organisation, including a cloud service provider, tell us about your hosting arrangement/s.

This question is to identify the location of your personnel and the location of the data handled under your data services.

The DATA Scheme requires that any personal information that is scheme data be held in Australia.

For the data services provided by your organisation, provide details of:

- the location of personnel; and
- a summary of your on-premise/s data storage.

If any of your data services will be hosted externally to the area providing data services, include details of:

- the name of your cloud and/or data centre provider/s;
- the data services being hosted; and
- level of privacy, sovereignty and security controls (where possible against the Commonwealth Hosting Certification Framework).

4.3 Tell us about the security roles in your organisation, including corporate role/s such as Chief Information Security Officer, and how these roles provide leadership and oversight of security including cyber in providing data services.

This question seeks to ensure security roles, responsibilities and accountabilities have been clearly documented, allocated and understood for your organisation and applied to the provision of data services.

For example, roles can include Chief Security Officer, Chief Information Security Officer, system owners, and system managers.

Refer to/attach the following:

- duty, role or responsibility statements of key security positions;
- security responsibilities chart, process flow or equivalent document; and

- representation of the relevant internal governance or security forums.

Explain how this leadership and oversight of cyber security is supported at the whole organisation level.

4.4 Outline your organisation's network management policies and activities that ensure:

- **secure network design and configuration;**
- **secure wireless networks; and**
- **service continuity for online services.**

This question seeks to ensure there are documented policies and processes, for the security networks associated with providing data services.

Refer to/attach the following:

- network design and configuration;
- network management policy or manual;
- network management process flow or diagram;
- how the computer network is isolated from the external environment or broader organisation; and
- explanation of how the Protective Security Policy Framework (or similar) is related to network management.

4.5 Outline your organisation's data storage system management policies and processes that apply to delivering data services and that ensure secure management of:

- **database servers;**
- **database management system software; and**
- **databases and other storage or file systems.**

This question seeks to ensure there are documented policies and processes for the confidentiality and integrity of systems and data.

Refer to/attach the following:

- database management documentation;
- database and system specific policies and processes;
- arrangements and processes for applying security classification protective markings; and
- explanation of how your application of security frameworks is related to database system management.

4.6 Tell us about your organisation's security plan, manual, policy or similar documents, including information on:

- **risks, threats and vulnerabilities that impact the protection of people;**
- **information and assets, security goals and strategic objectives;**
- **tolerance to security risks, assessment of maturity to manage security risks; and**
- **strategies to implement security risk management and maintain a positive risk culture.**

This question is looking to ensure robust security policies and processes are in place and endorsed by the appropriate senior management.

Refer to/attach the following:

- security, risk management or related policies;
- cyber security strategy, manual or related policies;

- ICT security strategy, manual or related policies;
- system specific security plans;
- information on security design standards;
- procedures for response to security risks or incidents; and
- evidence of your organisation's culture in responding to risks and threats.

4.7 Tell us about your organisation's software development policies and guidelines on a secure and consistent approach to application development including web application development.

This question is looking to ensure software development policies and guidelines provide a secure use of software.

For software developed or acquired for use in data services, provide details on how security risks are assessed and addressed before systems and applications are authorised for use, and throughout their operational life.

4.8 Tell us about your organisation's ICT equipment and media management policies and practices to ensure their controlled and secure usage.

This question is looking to ensure ICT equipment and media management policies, processes and procedures are in place for controlled and secure access to data.

Refer to/attach the following:

- permitted media usage policy or equivalent document;
- arrangements for repairs and maintenance, including outsource and contracting arrangements;
- collection and management of enterprise owned ICT equipment and media; and
- device sanitisation, destruction and disposal policies or similar documents.

4.9 Outline your organisation's controls to ensure mobile devices are securely managed and used appropriately.

This question is seeking to ensure controls are in place for mobile device security. Refer to/attach the following:

- enterprise mobility, mobile device or similar policy;
- bring-your-own-device or similar policy; and
- teleworking procedures for staff accessing or using data.

4.10 Tell us about your organisation's vetting processes or assessment when/if outsourcing information technology services.

This question is looking to ensure providers of outsourced information technology services are assessed for security risks and are contractually obliged to maintain appropriate security controls.

Refer to/attach the following:

- policy on use of external providers and specific organisations engaged;
- standard contracts or agreements used with external providers; and
- tender requirements for external providers.

4.11 Tell us about your organisation's policies and practices for system hardening, including operating systems, application and authentication processes.

This question is looking to ensure system hardening practices are in place and configured to reduce ongoing and emerging security risks.

Refer to/attach policies, protocols or manuals relating to system hardening.

4.12 Outline your organisation's system management policies and guidelines around:

- **secure system administration;**
- **system patching; and**
- **change management.**

This question is looking to ensure system management policies and guidelines are securely administered, maintained, developed and preserved.

Refer to/attach the following:

- information on system certification and approved ability to hold and share protected data;
- policies, framework or manuals relating to operating system management and configuration;
- policies and processes for managing accounts, access and authentication;
- data, information or digital preservation policy; and
- audit, review or incident reports related to the above.

4.13 Tell us about your organisation's data transfer policies and procedures.

This question is looking to ensure data transfer policies and procedures are clearly documented, consistent and understood.

Refer to/attach the following:

- documentation relating to data acquisition, extraction and provision;
- secure file transfer protocols;
- systems supporting large file transfers.

4.14 Outline your organisation's data encryption policies and procedures and their application in mitigating threats during the ingress and egress of data.

This question is looking to ensure cryptography policies and procedures are in place and up to date relating to data storage and transfer.

Refer to/attach, the following where available:

- Australian Signals Directorate Approved Cryptographic Algorithms and Protocols
- Transport Layer and Perfect Forward Security
- Secure/Multipurpose Internet Mail Extension
- Secure Shell (e.g. Secure Shell use, configuration, authentication mechanisms, automated remote access, and SSH-agent)
- Internet Protocol Security (e.g. mode of operation, protocol selection, key exchange, protocol modes, security association lifetimes, etc.)

4.15 Outline how your organisation achieves gateway monitoring for data movement into and out of your systems.

This question is looking to ensure gateway management policies and activities are in place. Refer to/attach the following:

- arrangements for gateway monitoring, including outsourcing;
- details of gateway access protocols and management;
- where available, use of
    - diodes;
    - web content filters (e.g. Transport Layer Security Filtering and inspection of traffic, allowing and blocking access to websites, etc.); and/or
    - peripheral switches.

4.16 Outline your organisation's system management policies and guidelines for data backup and restoration.

This question is looking to ensure system management policies and guidelines are securely administered, maintained, developed and preserved.

Refer to/attach the following:

- data backup and restoration policies and practices, including location of data backups;
- data, information or digital preservation policy; and/or
- audit, review or incident reports related to the above.

4.17 Outline your organisation's personnel security controls including:

- **ensuring individuals understand their security responsibilities and receive security awareness training including cyber;**
- **individuals have access to only what is required to do their job; and**
- **methods to identify and authenticate personnel.**

This question is looking to ensure robust processes for personnel security are in place.

Refer to/attach the following:

- recruitment security vetting processes;
- training and development policies and processes;
- processes for managing real and perceived conflicts of interest, and reporting changes in personal circumstances;
- workforce development or capability plan or similar document;
- cyber security, security policy and risk management or related training for staff;
- programs and activities to maintain staff awareness and vigilance related to security (e.g. notices, emails, newsletters, internal communication campaigns, etc.); and
- methods for controlled access policies or equivalent documents, including specific asset or system access arrangements relevant to data and projects.

4.18 Outline your organisation's physical controls to ensure the security of:

- **ICT equipment;**
- **wireless devices ; and**
- **facilities containing systems, servers, communications, security containers, network infrastructure and devices, and workspaces.**

This question is looking to ensure physical controls are in place to secure data. Refer to/attach the following:

- security policy relating to premises and associated physical access arrangements
- logging of physical access to premises;
- event monitoring and audits, including incident identification and analysis; and
- processes to ensure review of logs occurs.

4.19 Outline your organisation's system monitoring policies and analysis procedures and reporting for:

- **ongoing event logging;**
- **incident analysis; and**
- **auditing and review of logs.**

This question is looking to ensure system monitoring policies and analysis activities are in place and reviewed.

Refer to/attach the following:

- event logging policy;
- documentation of types of events identified and logged;
- event monitoring and audits, including incident identification and analysis; and
- processes to ensure review of logs occurs.

4.20 Outline your organisation's protocols, policies and practices to:

- **detect, manage, recover and report from security including cyber events/incidents; and**
- **respond and action security including cyber events/incidents in a timely manner.**

This question is looking to ensure protocols, processes and procedures have been established for cyber security events and incidents and appropriate responses to these.

Refer to/attach the following:

- business continuity or disaster recovery plan
- security incident or crisis management manual or similar document;
- security incident register;
- business continuity or disaster recovery tests; and
- security incident reporting protocols, policies or similar documents.

5. Skills and Capabilities

The following questions relate to your organisation's ability to demonstrate their technical capabilities and skills to protect, manage and use data and provide data services.

The responses are to provide evidence of policies, practices, skills and capability to perform the data services to be provided under the DATA Scheme.

Explanation of questions

5.1 Tell us about the experience the area providing the data service has had with access to government data or provided data services to government in Australia or internationally.

This question is seeking to understand your organisation's experience in handling government data.

Where relevant refer to/attach details of:

- your personnel involvement as users of government data requiring secure access and the environment used;
- your personnel involvement as a provider of government data requiring secure access;
- approved project proposals involving public sector data; and
- agreements with public sector data holders to provide data services.

Organisations that do not have experience with government data should provide details of equivalent experience that they have. Also refer the general guidance in this document addressing applications where you do not have prior experience.

5.2 Outline your organisation's data management policies and practices for the data services your organisation could provide.

This question is seeking to ensure data management documents are in place and endorsed by the appropriate senior management and implemented where the data services are provided.

Evidence that may be provided (additional to that provided at section 1) include:

- data management program, including policies and procedures covering the management of data over its lifecycle;
- data management chart, process flow or equivalent document specific to data services;
- data inventory, catalogue or register;
- data management or related training for staff;
- previous projects and/or experience demonstrating effective data management; and
- representation on relevant professional groups or forums.

5.3 Outline the key operational data roles, responsibilities and accountabilities, specific to each data service your organisation could provide.

This question is seeking to ensure key operational data roles, responsibilities and accountabilities have been clearly documented, allocated and understood. The focus in this question is the data roles directly involved in providing data services.

Refer to/attach details of:

- duty, role or responsibility statements of key data positions; and
- data operations areas organisational chart, process flow or equivalent documents.

Examples of roles are Data Linkage Manager, Principal Data Linkage Analyst, Senior Data Linkage Analyst, Senior Clerical Review Officer, Principal Data Analyst.

5.4 Tell us about your organisation's capability requirements, performance expectations and recruitment processes for data staff.

This question is seeking to ensure capability requirements, performance expectations and recruitment processes for data staff are clearly established.

Refer to/attach details of:

- skill, capability requirements and processes for recruitment of data positions, including position roles and descriptions;
- positions requiring specialist skills (e.g. staff undertaking the preparation and linking of data have suitable skills or experience to perform the work and apply robust statistical methodology);
- workforce development and capability plan or similar document, as relevant to data skills;
- details of relevant training or qualifications of staff (e.g. data science, mathematics, statistics, psychology, social science, etc.);
- data related training and development for staff; and
- data analysis software capability (e.g. SAS, SPSS, RStudio, Microsoft Excel or SQL, Stata, etc.).

5.5 Tell us about how your organisation will implement learning, development or training about the DATA Scheme for:

- **staff and**
- **customers.**

This question is seeking to ensure appropriate learning and development is in place, focusing on personnel undertaking data services.

Refer to/attach details of:

- staff learning and development plans;
- plans for skill acquisition for staff;
- customer data literacy and information resources;
- evidence that training will include:
  - handling personal information
  - privacy obligations
  - security processes e.g. handling a data breach, compliance with policy
- any staff working overseas.

Customers refers to users of your data services under the DATA Scheme, including other clients, researchers and analysts.

5.6 Outline your organisation’s metadata standards, classifications and/or interoperability policies and practices.

This question is seeking to ensure metadata standards, classifications and/or interoperability policies and processes are in place to maximise the utility of data.

Refer to/attach the following:

- adopted standards and classifications;
- interoperability manual, framework or similar document.

5.7 Tell us about your organisation’s data quality assessment policies and practices, including how these mitigate risk of misuse of data.

This question is seeking to ensure data quality is assessed and information made available to enable responsible data use.

Refer to/attach the following:

- mechanisms and frameworks for assessing data quality;
- data quality statements;
- publicly available and user information on data asset quality; and
- linkage project documentation demonstrating assessment of data quality.

5.8 Tell us about the policies, practices and roles your organisation has that support your technical skills and capabilities to meet the requirements of Data Sharing Agreements (DSAs) that relate to the role of an ADSP.

Data Sharing Agreements are a fundamental element of the DATA Scheme.

This question is seeking to ensure that your organisation has skills to provide data services as part of a DATA Scheme Data Sharing Agreement involving Data Custodian/s and Accredited Data Users.

Provide evidence to demonstrate governance and/or processes supporting your role as an ADSP engaging in DSAs. These should include:

- governance bodies and/or roles supporting your authorising officer when specifying data services in a DSA;
- internal procedures for quality assurance and approval of output or ADSP-enhanced data when data is shared; and
- where engaged as an intermediary in a DSA, ability to ensure compliance with the DATA Scheme.

5.9 Tell us about your experience adjusting settings, controls and constraints that will be relevant to meeting future requirements of Data Sharing Agreements.

This question is seeking to ensure when providing data services your organisation is able to adjust settings, controls and constraints to meet requirements set by Data Custodians in each Data Sharing Agreement.

Refer to/attach the following:

- previous projects requiring customised arrangements; and
- evidence of applying the data sharing principles in response to Data Custodian requirements and managing privacy risk.

5.10 Outline your organisation's capability to provide data integration services, including:

- **previous experience; and**
- **personnel skills and capability.**

This question to seeking to understand your organisation's capability to provide data integration services.

Refer to/attach the following:

- examples of approved data integration project proposals, including your role in joint data integration projects;
- details of experience with data integration projects;
- copies of, or links to, previous data integration projects, papers and outputs;
- details or copies of agreements with public sector data holders to provide data integration services; and
- profile of personnel skills and experience;

If your organisation is not intending to provide a complex data integration data service, please provide a statement that this data service is not intended to be provided instead.

5.11 Outline your organisation's data integration policies and practices.

This question is seeking to ensure data integration policies, processes and procedures are in place and endorsed by the appropriate senior management and in place in the area providing data services.

Refer to/attach, where relevant:

- data integration manual, operating guide, policies, methodology or similar documents;
- data linkage protocols, checklists, templates, forms and related documents; and
- data integration chart, process flow or equivalent document.

If your sub-unit is not intending to provide a complex data integration data service, please provide a statement that this data service is not intended to be provided instead.

5.12 How is the separation principle applied in your organisation's data integration structures and operations?

This question is seeking to ensure effective application of the separation principle in your organisation's data integration structures and operations.

The response to this question should include data integration process flow diagram/s or equivalent documentation.

This response may also include:

- functional separation (e.g. separation of data integration teams and/or roles, minimum staffing requirements for each integration project, etc.)
- external separation (i.e. Data Custodians provide separate linkage and content files)
- storage separation (e.g. holding linking, content, linkage key and merged data files on separate, access controlled servers), and
- analysis separation (i.e. analysts can only access the parts of integrated datasets relevant to their project).

5.13 Tell us about your organisation's experience providing secure access data services.

This question is seeking to ensure your organisation has experience with providing secure data access, including assessment of applicants, administration of user induction, training and confidentiality agreement processes, provision of secure transfer, on-site or remote access facilities, provision of data analytics software and appropriately treated microdata files, monitoring and auditing access sessions, and reviewing results and outputs.

Refer to/attach details of:

- current secure data access arrangements, including secure file transfer protocols, virtual, remote or on-site data laboratories;
- output vetting either automated or by appropriately skilled internal staff;
- previous experience creating appropriately treated microdata files to restrict inappropriate use of data;
- current processes for, and previous experiences of, managing authorised user selection, induction, training and confidentiality agreement processes;
- arrangements for recording, monitoring and auditing access sessions; and
- arrangements for releasing, vetting and managing dissemination and publication of results and outputs.

5.14 Tell us about your organisation's arrangements in providing secure access data service user support and training, including how users/researchers will interact with the data in your environment.

This question is seeking to ensure appropriate experience providing user support for secure data access.

Refer to/attach the following:

- guide or manual on use of data access arrangements;
- data and metadata catalogues, registries or inventories and guidance on their use;
- information on available software;
- information on user training provided and demonstration that staff have relevant skills and/or experience to deliver the training;
- query, complaints and requests mechanisms; and
- support services for user/researchers, such as clearing outputs or code, import functionality, linking, query management, expert advice, training.

If your organisation is not intending to provide secure access data service, please provide a statement that this data service is not intended to be provided instead.

5.15 Tell us about your organisation's data minimisation practices demonstrating your ability to apply this capability in data sharing projects.

This question is seeking to ensure effective data minimisation practices relating to your data services.

Refer to/attach, where available:

- policies and procedures ensuring only the data necessary for a project is received;
- procedures ensuring that only the data necessary for the project is held during the project; and

- policies and procedures ensuring only the data necessary for a project is made available to users.

5.16 Tell us about your organisation's policy, practices and experience treating data to manage disclosure risk.

This question is seeking to ensure your organisation has experience in treating data to manage disclosure risk and ensure re-identification, privacy/confidentiality breaches or other misuse (e.g. data being share outside the environment without knowledge of the data controller) does not occur.

Refer to/attach, where applicable:

- data dissemination and release policy or similar documents;
- confidentiality policy, processes or similar documents;
- confidentiality and output checking manual, guide, policies, processes or similar documents;
- details of arrangements for vetting, confidentialising and monitoring outputs;
- policies, processes and methodology for managing disclosure risk and de-identifying data (e.g. suppression, aggregation, perturbation, etc.); and
- policies and processes for managing data confidentiality breaches.

6. Consent and declaration

The consent and declaration section of the ADSP Application Form is required to be completed.

Refer to the Instructions for making an ADSP application for details on how to submit your organisation's application.