Australian Government
Office of the National Data Commissioner

ONDC

Sample User Accreditation Form

This sample application incorporates all the questions that may appear in the online accreditation application form, together with guidance to help you to complete the form. The online application form is available on the Dataplace portal.

This sample application may be useful if you are responsible for developing or coordinating your organisation's application.

The online application looks different from this sample as it operates as a series of screens. In addition, you may not be asked all questions in the sample application because the online form tailors the visible questions to your responses.

Warning

This is a sample application provided for information purposes only.

To lodge an application for user accreditation under the DATA Scheme, use the online form available on Dataplace.

Introduction

Organisations that wish to request Australian Government data under the Data Availability and Transparency Act (DATA) Scheme, or organisations who wish to provide specialist data services under the Scheme, must become accredited. You can find more information about the DATA Scheme, including about the two types of accreditation, on the **ONDC website**.

Organisations that wish to become an Accredited User (also referred to as an accredited data user) under the DATA Scheme are able to apply by completing the application form below.

The application process for organisations interested in becoming an ADSP will open 1 August 2022.

To become an Accredited User we will ask for information to help us assess that you have:

a) appropriate data management and governance policies and practices and an appropriately qualified individual in a position that has responsibility for data management and data governance for the entity.
b) the ability to minimise the risk of unauthorised access, sharing or loss of data.
c) the necessary skills and capability to ensure the privacy, protection and appropriate use of data, including the ability to manage risks in relation to those matters.

When completing the application form, you may need to seek information from multiple areas within your organisation. The information you will need to provide covers the following topics: IT, such as cyber security controls; HR and learning and development, such as training and on-boarding processes; and data governance including your data management practices.

Before you start the application form you should run through the User Accreditation Application Checklist to help you prepare.

Note that **if two users are editing the online form at the same time, the last person who saves will overwrite the current content.**

There is guidance material provided throughout the form and you can also download the form and guidance for reference. You can save the form and come back to it as many times as necessary prior to submission.

Where you provide personal information in this application, ensure you have obtained consent from those individuals.

Organisation details

#	Questions	Response field	Help text
1.1.	Name Type of entity ABN /ACN Legal name of the organisation	*Prefilled*	If your organisation details are incorrect, please contact the ONDC.
1.2.	Provide an email/emails for general enquiries	Inbox 1 Inbox 2	We recommend selecting group mailboxes as this will be available to the public and used for formal notices. These may be updated at any time from the manage organisation section of Dataplace.

Authorised officer

#	Questions	Response field	Help text
1.3.	Who is the authorised officer making the application for accreditation on behalf of your organisation?	• I am the authorised officer • Other First Name Last Name Preferred name Email Phone Position title	The accreditation application must be submitted by an authorised officer. Only certain people can be an authorised officer, as defined in the DAT Act (section 137).

Contact officer

This is the person the ONDC will contact if we have any questions about the application, or if we require further information. If you nominate someone other than the authorised officer, the ONDC will contact that person as needed, but will also copy in the authorised officer to correspondence.

#	Questions	Response field	Help text
1.4.	Would you like to nominate another individual to be a contact point for the accreditation process?	• No – The authorised officer above will be the main contact. • Yes - The individual listed below will be the main contact. If yes – display:	

#	Questions	Response field	Help text
		First Name Last Name Preferred name Email Phone Position title	

About your organisation

This section of the application provides contextual information about your organisation that can help the ONDC assess your organisation's capability against the accreditation criteria.

#	Questions	Response field	Help text
1.5.	Does your organisation have any obligations or affiliations that could impact or conflict with obligations under the DAT Act should your organisation become accredited?	• Yes • No If yes - How will you manage these matters to ensure compliance with the DAT Act? *[free text]*	When you are accredited to participate in the DATA Scheme your organisation will have obligations to keep the data safe. 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 foreign members of your organisation and any standard access they may have to data and data projects • any other relevant foreign influences.
1.6.	What is the nature of your organisation's business and how would access to Commonwealth government data support that?	Free text *(250 word limit)*	Provide a brief statement about what your organisation does, how you use data and why you seek access to Commonwealth government data. Commonwealth government data can only be shared under the DATA Scheme for projects that are in the public interest and for purposes defined in the DAT Act. The purposes defined in the DAT Act are: • delivery of government services;

#	Questions	Response field	Help text
			• informing government policy and programs; and • research and development. Please note that your response to this question may be published on a register of DATA Scheme participants and/or on your organisation profile.
1.7.	What is the approximate size of your organisation?	• Small (1 - 19 employees) • Medium (20 – 199 employees) • Large (200 - 999 employees) • Extra large (1000 or more employees)	Provide a general estimate that includes all employees, including those who are on contracts or casual.

OFFICIAL

Criteria

Criterion 1: Data Management and Governance

This section of the application provides information about:

- the nature of data your organisation manages
- your organisation's data management and governance policies and practices, and
- that your organisation has an appropriately qualified individual with responsibility for leading the organisation's data agenda.

Applications will be assessed in the context of the size of your organisation and your organisation's experience with data. While the questions are specific to each criterion, your application will be assessed as a whole against the criteria in the DAT Act.

We do not expect all organisations to necessarily have all elements covered in the questions below. Organisations will tailor their data management and governance practices according to the role that data plays in their organisation, the type of data they work with and the nature of their business. There are opportunities in the questions to provide commentary about your data management practices to contextualise your responses.

#	Questions	Response field	Under question text
	Organisational data holdings The following questions ask about the nature of data your organisation manages.		
2.1	What is the volume of your organisation's data holdings?	Number Comment (optional) *[free text]*	Provide an estimate in Terabytes. Please include your organisation's business data, such as data relating to clients, business activities and operations. Do not include your own corporate (e.g. HR or financial) data. Do not include data contained in archives and backups or any other duplicates. Provide comments to add to your response if useful.

OFFICIAL

2.2	How much of your organisation's data is treated as sensitive?	• A little (0 – 15%) • Some (16 - 50%) • Most (50 – 100%) • Unsure (comment) *[free text]*	What is considered sensitive can be context specific. Sensitive data can include information that is personal, commercially, environmentally or culturally sensitive. For the purposes of this application form, the Protective Security Policy Framework (PSPF) Policy 8: Sensitive and classified information should be used to help you consider whether the data referred to is sensitive data. This requires organisations to assess the value, importance or sensitivity of information and the potential damage to government, the national or public interest, organisations or individuals that would arise if the information's confidentiality was compromised. In addition, sensitivity of data should be considered where data relates to culture of people and the environment. This is different to the technical meaning of 'sensitive information' within the *Privacy Act 1988*, which refers to a subset of personal information. We understand that the definition of sensitive is subjective and will depend on the context where the data is applied. Please consider the impact if the information is compromised to determine whether the data you hold is sensitive.
2.3	What subject matter data does your organisation hold?	□ Economy (e.g. Labour, Business, Industry, Financial) □ Society (e.g. Population, Migration, Culture, Health, Education, Crime and Justice, Disability, Aboriginal and Torres Strait Islander Peoples) □ Environment (e.g. Land, Water, Atmosphere, Biodiversity) □ Other (describe) *[free text]*	

2.4	How much of your organisation’s data is created in or by your organisation?	• A little (0 – 15%) • Some (16 – 50%) • Most (50 – 100%) • Unsure (comment) *[free text]*	Data created in or by your organisation is any original data collection by your organisation (e.g. through a survey or data manipulation) or collected by your organisation because of business processes that it manages (e.g. applications for a permit). This distinguishes from data that has been collected by other organisations. The percentage of data is relative to the estimated volume of data holdings you provided above.
	Organisational data governance controls The following statements refer to your organisation’s data management and governance policies and practices and that your organisation has an appropriately qualified individual with responsibility for leading the organisation’s data agenda.		
2.5	We know the data we hold	• We do not have any kind of organised inventory of our data holdings • We have an inventory of the personal information that we hold • We have a number of different data inventories, including an inventory of personal information although nothing centralised • We have a centralised data inventory, which includes personal information Comment (optional) *[free text]*	
2.6	We know the value of data that we hold	• The value of data held by our organisation is unknown • The value of data is driven by the needs of projects and/or individuals • Business units understand the value of the data they hold (e.g., could identify business critical data/high value data quickly) • We understand the value of our data at an organisational level and have a consistent way of assessing the value of individual datasets to the organisation Comment (optional) *[free text]*	

2.7	We manage data that we hold	• We have no established practice for managing data • Our data is managed for a single purpose or on a project-by-project basis, by individuals according to their time and capability or by business units with some established practices • Our data is managed according to practices defined and documented at the organisational or business unit level as relevant • Our data is managed according to its value; we have a consistent way of valuing data across the organisation and invest proportionate effort in its management (i.e., set management standards according to high and low value data) Comment (optional) *[free text]*	
2.8	We manage our metadata*	• We have no defined metadata standards • We have some defined metadata standards • We have agreed metadata standards defined for most data • We have agreed metadata standards defined for nearly all data Comment (optional) *[free text]*	*metadata – Other data standards are considered in later questions.
2.9	We use data ethically	• Our work does not require consideration of ethics • We do not have a process for the consideration of ethics in using data • We have a clear framework for the organisation to consider ethics associated with using data • We are bound by policy or legislation to consider ethics Comment (optional) *[free text]*	

2.10	We have monitoring and reporting arrangements in place to govern our data management and use	• There is no regular or systemic monitoring or reporting arrangements in place • There is informal, project-based monitoring and reporting arrangements in place • There is organisational monitoring and reporting arrangements in place with limited review mechanisms • There is organisational monitoring in place and a senior manager responsible for reporting and review to an executive committee Comment (optional) *[free text]*	
2.11	We have incident management arrangements in place to govern our data management and use	• There is no structured approach to incident management and/or breach response • There are informal incident response processes managed on a project basis or within business units • We have an incident management response plan with clear and documented incident response and escalation procedures • We have an incident management response plan which is regularly tested and continuously improved Comment (optional) *[free text]*	Your incident management plans may include but not limited to: • data breach mitigation plan • disaster recovery plan • business continuity plan More information on incident management can be found in [PSPF Policy 10: Safeguarding information from cyber threats].

2.12	We manage data risks	• There is no risk management strategy in place • There is a general risk management strategy in our organisation • The business areas are responsible for managing their data risks within the organisational risk management strategy • There is an organisational wide approach to managing data risks • The organisation reports data risks to an external body, including the public Comment (optional) *[free text]*	
2.13	Does your organisation have obligations for handling personal information?	• Yes – legislative obligations • Yes – policy obligations* • No Comment (optional) *[free text]* If Yes - legislative, What legislation applies to your organisation? □ *Privacy Act 1988* (Cth) □ *Information Privacy Act 2014* (ACT) □ *Privacy and Personal Information Protection Act 1998* (NSW) □ *Information Act 2002* (NT) □ *Information Privacy Act 2009* (QLD) □ *Privacy and Data Protection Act 2014* (VIC) □ *Personal Information Protection Act 2004* (TAS)	This includes how you collect, store and use personal information. * Yes – policy obligations – You may have a whole of government or agency specific policy that you commit to.

2.14	How does your organisation manage personal information?	□ We do not deal with personal information □ We have a privacy policy for the organisation □ We have position specific privacy policy/policies □ We have guidance material, checklists and templates that informs how to manage privacy and respond to incidents □ We have an ethics framework that includes consideration of how we seek consent and how we use personal information □ We have mechanisms in place to ensure informed consent for the data that the organisation receives/uses □ We have mandatory privacy training (including compliance checks) □ We regularly consider the privacy impacts of any new projects and systems that involve personal information and undertake Privacy Impact Assessments when needed □ We have assurance activities to drive improvement in how we manage privacy obligations □ Other (Comment) – *[free text]*	For this question, 'personal information' only includes client/customer/business data. This does not include corporate or HR data.

2.15	What data management/governance roles does your organisation have?	□ Chief Data Officer (CDO) – Accountable for enterprise-wide governance and use of data as an asset within an agency. □ Chief Analytics Officer – Oversees an agency’s analytics function, including data analytics and data science. □ Chief Information Officer (CIO) – Oversees the inward view of technology in an agency. □ Chief Technology Officer (CTO) – Oversees the outward view of technology in an agency. □ Chief Information Security Officer (CISO) – Ensures the alignment of cyber security and business objectives in an agency. □ Chief Information Governance Officer (CIGO) – Establishes and maintains an enterprise-wide culture for an accountable and business-focused information management environment. Often performed by CDO or CIO. □ Data Stewards – Oversees day-to-day management of data collected and held by an agency within a defined data domain or business area. Sometimes referred to as Domain Data Stewards. □ Data Champion – Promotes best practice use, sharing and re-use of data within their agency and across the APS. □ Privacy Champion – Promotes a culture of privacy that values and protects personal information within an agency. □ Privacy Officer – Promotes a strong privacy governance and capability within an agency.	

		□ Other (Comment) *[Free text]*	
2.16	Who is the person chiefly responsible for the data management and data governance of your organisation?	Full Name	This person should be in one of the roles identified above.
2.17	Provide a brief summary of the qualifications, skills and experience of the person chiefly responsible relevant to their data management and data governance role.	*[Free text]*	Please limit the response to 100 words or 3 dot points.
2.18	Please upload a description of the role and responsibilities of the person chiefly responsible for data management and data governance.	Choose file	

2.19	What data management and governance documents does your organisation have?	Name of policy/document/guideline - *[free text]* Describe what it covers - *[free text]* How is it published? • Published/accessible internally to select staff • Published/accessible internally to all staff • Published internally and externally How is it communicated to staff? • Areas are responsible for ensuring new staff are aware of it • There is communication to remind/educate all staff about it at least once a year • Training/education is provided to new staff when they join (on-boarding processes) • There is a specific training program available to staff How is it reviewed/updated? • It is not periodically reviewed • It is periodically reviewed and updated although there is no engagement by staff in the review • It is periodically reviewed and updated by a governance body with staff engagement How is it enforced? • There is no monitoring or enforcement of the policy • Checks are done to ensure staff are aware of the policy • Checks are done to ensure staff are aware and complying with the policy	Provide information about the documents your organisation has on its data management and governance practices. This may include data strategies, policies, data handling procedures, data governance frameworks, risk management, ethics, and audit programs. If your documentation is extensive, provide details for up to 10 most relevant documents that, collectively, showcase your organisation's approach to data management and its governance. Please consider also which documents support your responses to other questions in this form. If you have more than 10 documents, only provide the title of remaining documents.
2.20	Having regard to the list of documents set out above, please upload the document that is most relevant to your organisation's data management and data governance policies.	Choose file	

2.21	What governance bodies related to data, risk management and/or audit does your organisation have?	Name of governance body What is the key function/responsibility of the body, including any monitoring programs that report to the body? - *[free text]* Are there requirements on who can be the chair (e.g. by seniority or by defined position)? • Yes • No What is the composition of membership? • All internal members • Mix of internal/external members Are members required to have specific skills or qualifications or roles? • Yes • No	If your list of governance bodies is extensive, please provide details for up to 10 most relevant governance bodies across the organisation. Please consider which governance bodies would support your responses to other questions in this form. If you have more than 10, only provide the name of remaining governance bodies.
2.22	How will your organisation manage and govern your DATA Scheme obligations?	Free text	

Criterion 2: Security Settings

This section of the application provides information about:

- how your organisation proposes to store the data accessed through the DATA Scheme
- your organisation's approach to minimise the risk of unauthorised access, sharing or loss of data, and
- your organisation's data transfer, storage and disposal controls.

We do not expect all organisations to necessarily have all elements covered in the questions below. Organisations will tailor their security practices according to the role that data plays in their organisation, the type of data they work with and the nature of their business. There are opportunities in the questions to provide commentary about physical and cyber security practices to contextualise your responses.

#	Questions	Response field	Help text
	Organisational DATA Scheme data storage The following questions ask about how your organisation proposes to store the data accessed through the DATA Scheme.		
3.1	Does your organisation plan to store and manage data accessed through the DATA Scheme on your IT network(s)?	• Yes – *(continue)* • No – Your accreditation will include a condition that you cannot host data accessed through the DATA Scheme. *(end of security section)*	You may not be planning to store data accessed under the DATA Scheme on your IT networks. This may be because you are planning to use using an ADSP's secure data access service or for other reasons. The ADSP secure data access service provides a secure environment where users can do their data analysis.
3.2	How many network(s)* does your organisation manage?	Number	*network(s) - A group of self-contained infrastructure (including workstations, servers, devices etc.) which your organisation controls, operates and manages with appropriate security controls and ICT policies and procedures in place.
3.3	Does your organisation have a Protected network/networks?	• Yes – Our organisation manages its own Protected network *(continue)* • Yes – Our Protected network is provided by a different organisation *(continue)* • No – *(go to question 3.6)*	A 'Protected network' is as defined by the Protective Security Policy Framework (PSPF).

3.4	Does your organisation intend on only storing data accessed through the DATA Scheme on your Protected network(s)?	• Yes – Provide a name for the location where data accessed through the DATA Scheme will be stored – *(continue)* • No – Please only answer the following questions for your networks which are not rated to Protected. – *(go to question 3.6)*	
3.5	Does your organisation's Protected network(s) have secure and encrypted communication/transfer capabilities?	• Yes - *(end of security section)* • No/Unsure – *(only display question 3.19 - end of security section)*	
3.6	Where will your organisation store, use, analyse and manage data accessed through the DATA Scheme?	Name (e.g. Internal staff network) - *[free text]* Hosting provider for the data centre (e.g. Amazon Web Services) - *[free text]* Hosting data centre location (e.g. Moorebank, Sydney) - *[free text]* Status under the Digital Transformation Agency's Hosting Certification Framework a. Uncertified Provider b. Certified Assured Hosting Provider c. Certified Strategic Hosting Provider	Include the location(s) of any back-ups or archives that will be kept. If you rely on third parties to provide or manage your IT network, this should be included in the Hosting provider for the data centre. If you have your own on premise data storage, include your organisation name and details as the answers to these questions.
	Organisational security settings The following questions ask about your organisation's approach to minimise the risk of unauthorised access, sharing or loss of data and your organisation's data transfer, storage and disposal controls.		

3.7	Which of the following are in place in your organisation?	□ Information classification markings □ Security risk owners, stewards or managers □ Security policy or plan □ ICT Security policy or plan □ Security investigation and response plan or processes □ Security incident monitoring plan □ Security incident response plan □ Security governance for contracted goods and service providers (e.g. standard clauses about access or breach notifications) □ Security reporting processes (e.g. concerning or unexplained behaviour from colleagues) □ Specific role responsible for security (e.g. Chief Security Officer) □ Security assurance and review processes □ Security committee or forum □ Security risk management framework	

3.8	Which of the following has your organisation been assessed against in the last 12 months or is a part of currently?	□ Protective Security Framework Maturity Self-Assessment – *[free text]* □ Essential Eight Maturity Assessment – *[free text]* □ Information Security Registered Assessor Program Assessment – *[free text]* □ Australian Competition and Consumer Commissioner Consumer Data Right Accreditation – *[free text]* □ Information Security Management System (ISMS)/Organisational Protective Security Framework – *[free text]* □ ISO27001:2013 Information Security Management (ISMS) – *[free text]* □ NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organisations: A System Life Cycle Approach for Security and Privacy – *[free text]* □ Payment Card Industry Data Security Standard – *[free text]* □ ACSC partner* – please describe explain your partnership level *[what level]*	For each selected, please include a brief assessment outcome in the associated free text field. For example, a summary of the assessment outcome for the Essential Eight Maturity Assessment would include the Maturity Level achieved. * ACSC partner - The ACSC Partnership Program enables Australian organisations and individuals to engage with the ACSC and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy.

3.9	What physical security settings are in place in your organisation?	□ Restricted building access (e.g. keys, swipe access or sign-in) □ Restricted visitor access (e.g. sign-in and escort) □ Lockable offices □ Secure storage facilities (e.g. locked cabinets) □ Restricted access to server and communications rooms □ Separation of workspaces (e.g. privacy screens or cubicles) □ Permanent security presence (e.g. patrols and monitoring) □ Remote or teleworking arrangements □ Closed-circuit television (CCTV) □ Automatic removal of individuals' physical access after cessation with organisation □ Other (Comment) – *[free text]*	If your organisation has multiple physical locations, only include measures which are applicable across all locations.
3.10	What application controls for workstations and servers are in place in your organisation?	□ Organisation approved application control rule sets (e.g. restrictions on executables, software libraries scripts, installers, compiled HTML, HTML applications, control panel applets and drivers) □ Vendor recommended block rules □ Vendor recommended driver block rules □ Validation of application control rule sets at least annually □ Other (Comment) – *[free text]*	

OFFICIAL

3.11	What application patching controls are in place in your organisation?	□ Application of security patches, updates or vendor mitigations in internet-facing application services □ Application of security patches, updates or vendor mitigations for software, browsers, emails and security products □ Application of security patches, updates or vendor mitigations for other applications □ Vulnerability scans for internet-facing services daily □ Vulnerability scans for software, browsers, emails and security products at least weekly □ Vulnerability scans for other applications at least fortnightly □ Applications are removed when no longer supported by vendors □ Other (Comment) – *[free text]*	
3.12	What operating system patching controls are in place in your organisation?	□ Application of operating system security patches, updates or vendor mitigations for internet-facing services □ Application of operating system security patches, updates or vendor mitigations for workstation, services and network devices □ Vulnerability scans for operating system internet-facing services daily □ Vulnerability scans for workstations, services and network devices at least weekly □ Latest or previous release of operating systems used for workstations, servers and network devices □ Operating systems that are no longer supported by vendors are replaced □ Other (Comment) – *[free text]*	

3.13	What user application hardening controls are in place in your organisation?	□ Users cannot change web browser or software security settings □ Web browsers do not process Java from the internet □ Web browsers do not process advertisements from the internet □ Blocked PowerShell script executions are logged □ Vendor or Australian Cyber Security Centre hardening guidance on web browsers is implemented □ Vendor or Australian Cyber Security Centre hardening guidance on Microsoft Office is implemented □ Vendor or Australian Cyber Security Centre hardening guidance on PDF software is implemented □ Other (Comment) – *[free text]*	
3.14	What setting configuration controls are in place in your organisation?	□ Users cannot change macro security settings □ Macros are disabled where not required □ Macros originating from internet files are blocked □ Macros can only execute when originating from a trusted source □ Macro antivirus scanning is enabled □ Macros are blocked from making Win32 API calls □ Macro executions are logged □ Management of macros is restricted to privileged users □ Trusted publishers are validated at least annually □ Other (Comment) – *[free text]*	

3.15	What restrictions on administrative privileges are in place in your organisation?	□ Separate privileged and unprivileged operating environments □ Unprivileged accounts cannot log on to privileged operating environments □ Privileged accounts cannot log on to unprivileged operating environments (excluding local administrator accounts) □ Validation of privileged access requests □ Multi-factor authentication for privileged users □ Privileged accounts can only access what their duties require □ Privileged accounts are prevented from accessing the internet (excluding privileged service accounts) □ Automatic suspension of privileged accounts after a period/ inactivity □ Revalidation requirements for privileged accounts after a period □ Privileged account access is logged □ Privileged account and group changes are logged □ Use of jump servers for administrative activities □ Other (Comment) – *[free text]*	

3.16	What user restrictions and authentication arrangements are in place in your organisation?	□ Access control lists □ Unique access/logins □ Automatic removal of user accounts after cessation with organisation □ User accounts can only access what their duties require □ Automatic suspension of user accounts after a period/inactivity □ Revalidation requirements for user accounts after a period □ Multi-factor authentication for users □ Multi-factor authentication for users accessing important data repositories □ Validation of requests for access to data (e.g. need-to-know) □ Verifier impersonation resistant multi-factor authentication □ Access attempts are logged □ Other (Comment) – *[free text]*	
3.17	What incident response arrangements are in place in your organisation?	□ Intrusion detection and prevention policy □ Trusted insider detection and prevention plan □ Security personnel have access to sufficient tools to monitor for compromise □ Data access is restricted when a spill occurs □ Infected systems are isolated, scanned and the infection removed □ Incident support is available 24x7 □ Timely post-incident analysis is undertaken □ Cyber security incidents are reported to the ACSC □ Other (Comment) – *[free text]*	

3.18	What ICT equipment management processes are in place in your organisation?	□ Physical destruction of IT media □ Device management and maintenance program (e.g. hardware repair or equipment register) □ ICT equipment sanitisation and disposal management program including processes and procedures and assurances □ Data and archiving disposal processes, procedures and assurances □ MFD print drums, printer ribbons are destroyed at end of use □ USB and peripheral ports are removed/disabled for users □ Exit settings on clipboard, screen captures, USB devices are locked while using applications □ External storage units are encrypted, secured and password protected when not in use □ Other (Comment) – *[free text]*	
3.19	What cryptography arrangements are in place in your organisation?	□ Encryption of data at rest □ Encryption of data in transit □ Encryption software that has completed an ASD Cryptographic Evaluation □ Use of ASD Approved Cryptographic Algorithms (AACA) □ Use of ASD compliant High Assurance Cryptographic Equipment (HACE) □ Use of ASD Approved Cryptographic Protocols (AACP) to communicate data □ Separate and secure storage of cryptographic equipment □ Encryption key management, including generating, using, storing, archiving and deleting of keys □ Other (Comment) – *[free text]*	

3.20	Are your organisation’s data backups and archives encrypted, password protected and physically secured?	• Yes • No	
3.21	Does your organisation have any other security arrangements relevant to data sharing?	• Yes – *[free text]* • No	For example: secure data transfer protocol, cryptography, secure data warehouse, use of ACSC evaluated products etc.

Criterion 3: Skills and Capabilities

This section provides information about your organisation's:

- previous experience with seeking government data
- skills and capability to ensure the privacy, protection and appropriate use of data, and
- ability to manage risks in relation to privacy, protection and use of data.

We do not expect all organisations to necessarily have all elements covered in the questions below. Organisations have different data skills and capabilities according to the role that data plays in their organisation. There are opportunities in the questions to provide commentary about your data management practices to contextualise your responses.

#	Questions	Response field	Help text
	Organisational government data experience The following question asks about your organisation's previous experience with seeking government data.		
4.1	Has your organisation sought access to government data in the last five years?	• Yes • No If yes – What organisation did you seek data from? – *[free text]* Type of data sought □ Economy (e.g. Labour, Business, Industry, Financial) □ Society (e.g. Population, Migration, Culture, Health, Education, Crime and Justice, Disability, Aboriginal and Torres Strait Islander Peoples) □ Environment (e.g. Land, Water, Atmosphere, Biodiversity) □ Other (describe) *[free text]* What was the data classified? • Unsure • Unofficial • Official • Official sensitive • Protected Did the project go ahead?* • Yes • No • Comment – *[free text]*	We are seeking to understand if you have experience with requesting government data. If your experience is extensive, provide only the three most relevant projects, prioritising Commonwealth government data requests. * Did the project go ahead? - A request and refusal to access data will not result in an automatic refusal of accreditation under the DATA Scheme.

	Organisational skills and capabilities The following questions ask about your organisation's skills and capability to ensure the privacy, protection and appropriate use of data and ability to manage risks in relation to privacy, protection and use of data.		
4.2	What data roles does your organisation have?	□ Data analyst – investigates data, gathers insights and conveys findings □ Data broker – works with data integration teams, report writers, data analysts etc. to access the data they need to meet their objectives □ Data engineer – gathers data, organises and maintains databases □ Data manager – develops systems, procedures and policies for data management □ Data scientist – applies statistical techniques to data, gathers insights and conveys findings □ Data policy/governance – defines standards and management practice and assist in governing the organisation's data activities □ Other (describe) – *[free text]*	The terms used here may be different to those used in your organisation. We are seeking to understand whether your organisation have dedicated employees performing data functions. You may define your own terms.
4.3	Of the roles identified above, what percentage are employed on a casual/temporary/short term basis?	• A little (0 – 15%) • Some (16 - 50%) • Most (50 – 100%) • Unsure (comment) *[free text]*	
4.4	Are any individuals in those roles working overseas?	• Yes • No Comment (optional) *[free text]*	
4.5	Our staff can seek guidance on data analytics	• There is no formal organisational/support structure (individuals check with colleagues and external sources) • There is a centralised data analytics team within our organisation • There is data expertise embedded across the organisation	

		- There are practices in place to regularly review and perform quality assurance of outputs, although this may not be every project Comment (optional) [free text]	
4.6	We commonly manipulate data using	□ Preparatory techniques such as data cleaning and imputation □ Transformative techniques such as formatting and recodes □ Confidentiality techniques such as suppression and rounding □ Other (describe) - *[free text]*	
4.7	We commonly analyse data by	□ Using outputs from data analysis software packages □ Producing meaningful exploratory information about a data set, such as summary statistics and charts □ Undertaking first order analysis on a data set using techniques such as hypothesis testing or linear regression □ Undertaking higher order analysis on a data set using advanced techniques like logistic regression, ARIMA modelling or spatial analysis □ Other (describe) - *[free text]*	
4.8	We commonly communicate and describe data by	□ Describing the sorts of research questions the data can help answer □ Giving meaning to the results of any data analysis conducted □ Producing clear and understandable data visualisations using the data □ Conveying simple yet compelling arguments to make changes based on the data □ Other (describe) - *[free text]*	
4.9	What workforce management processes related to data are in place in your organisation?	□ Future skills planning □ Ongoing support for capability uplift □ Funding professional memberships	

		☐ Other (describe) - *[free text]*	
4.10	What workforce vetting processes are in place in your organisation?	☐ Identity check* ☐ Reference checks ☐ Qualification verification ☐ Citizenship check ☐ Police check ☐ Financial background check ☐ Security clearance* requirements ☐ Conflict of Interest* and/or anti-fraud policies including association or affiliation with a government, political party, government owned enterprise, military or police organisation in a country other than Australia ☐ Other (describe) - *[free text]*	Only select those that apply to all employees. *Identity check - Identity checks should be Australian Standard AS 48112006 (Employment screening) and the Standards Australia publication HB 323-2007 (Employment screening handbook). *Security clearance - Security clearances should be monitored if roles change. *Conflict of interest - There should be mechanisms to retest conflict of interest for discrete projects the organisation manages.
4.11	What learning, development or training related to data does your organisation offer?	Name of offering - *[free text]* Description of what it covers - *[free text]* How is it presented? • Self-directed learning • Facilitated learning, either face-to-face or face-to-screen • Blended model Is it mandatory? • Yes – all staff • Yes – identified staff • No How is it reviewed/updated? • It is not periodically reviewed and updated • It is periodically reviewed and updated although there is no engagement by staff in the review • It is periodically reviewed and updated by a governance body/targeted group • It is periodically reviewed and updated and the organisation is invited to participate in the review/able to provide feedback	Please provide information on the training available to staff regarding data, including data analysis, data ethics, privacy awareness, security awareness, security, cyber security, records management, data handling, risk management, fraud, and foreign interference. If your learning, development and training offerings are extensive, please limit responses to the 10 most relevant offerings across the organisation. Please consider which offerings would support your responses to other questions in this form. If you have more than 10, please provide the name of additional/specialist/subject area offerings.

		How do you assess the uptake of the training? • There is no monitoring or enforcement of the activity • Completion is recorded • Records of completion rates are checked and incomplete activities are followed up Are staff required to undertake regular refresher courses? • Yes • No	
4.12	Will your organisation create new learning, development or training about the DATA Scheme if you are accredited?	• Yes • No	
4.13	Which off boarding or termination processes are in place in your organisation?	□ Removal of data permissions and access □ Controls to prevent the removal of information from secure systems □ Decommissioning of email addresses, remote access, usernames and swipe cards □ Collection of access cards and remote access tokens if applicable □ Collection of organisation managed devices □ Process to ensure intellectual property and paper files are recovered □ Other (describe) - *[free text]*	This includes by transfer to a different role within the organisation.

Consent and declaration

This section is mandatory before the application can be submitted.

Only the authorised officer may submit this application. If you are not an authorised officer, you can send a notification to the authorised officer informing them that the application is ready for submission.

I consent to the Commissioner and, if the Minister is the accreditation authority for this application, the Minister, and any person assisting with assessing this application, including any person acting as a delegate of the Commissioner or the Minister:

- obtaining information relevant to this application from third parties, and
- verifying information with third parties in support of this application.

I declare that:

- I am an authorised officer of the Applicant and have authority to make this application on behalf of the Applicant, in accordance with section 76 and 137 of the *Data Availability and Transparency Act 2022*.
- Information provided in this application, including any attachments, is correct.
- Individuals have consented for their personal information to be included in this application.
- I understand that the Applicant will be required to comply with the obligations of an accredited user and any conditions of accreditation that may be imposed by the accreditation authority, if accredited under the *Data Availability and Transparency Act 2022*.

NOTE

It is a serious criminal offence under the Commonwealth *Criminal Code* to knowingly provide false or misleading information to a person exercising a function under any law of the Commonwealth, including the *Data Availability and Transparency Act 2022*. Providing false or misleading information in an application (including any omission of a matter without which the information is misleading) may also be grounds to suspend or cancel any accreditation granted on the basis of that information.