Expected characteristics for user accreditation

This information has been developed to assist organisations when preparing an application for user accreditation. It provides information about the expected characteristics for accreditation of users under the DATA Scheme.

Expected characteristics

One of the requirements under section 74 of the Act is that the applicant meets the criteria in section 77(1) of the Act, to a standard appropriate for accreditation. The characteristics, as set out below, inform the expectation against which these criteria will be assessed. The accreditation authority will be guided by these characteristics but will exercise their discretion for each decision.

While the characteristics inform each of the criteria under section 77, some characteristics are present in more than one criterion and the criterion support each other. Under these characteristics, policies and practices should be current, regularly communicated to staff, regularly reviewed, updated, and actioned (for example through awareness, monitoring and reporting).

In addition to assisting entities prepare an application for user accreditation, considering the expected characteristics may also be beneficial in informing enterprise-wide action planning, development, or maturity improvement programs.

Please read this information in conjunction with the User Accreditation Application Checklist (pdf) and other guidance available at www.datacommissioner.gov.au. This information is not intended to be legal advice. You should seek your own legal advice if you would like further clarification on the matters raised.

You can contact us at information@datacommissioner.gov.au if you have any queries.

Data management and governance policies and practices, and a qualified individual

The entity has 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 (s 77(1)(a) of the Act), evidenced by:

1. Identified role/s responsible for the organisation's:
   - data management and data governance (Chief Data Officer or equivalent)
   - information and communications technology, including security (Chief Information Officer or equivalent); and
   - management and governance of personal information (Privacy Officer or equivalent).
2. A governance body or bodies responsible for:
   - overseeing the organisation's data management and governance
   - monitoring and reporting of data management and use

- managing data risks; and
- audit.

3. Organisational policies and practices that document roles, responsibilities and processes for managing and governing data.

   These may be contained in one or more documents, but must include:

   - a high level strategy (e.g., data strategy, data governance framework)
   - policies and procedures that address:
     - a defined way of knowing what data is held (e.g., data inventory)
     - identification of data assets containing business-critical, personal or sensitive information (data value)
     - established practices for managing data, including agreed metadata standards.
   - a risk management strategy (or equivalent) that considers data risks
   - a data incident management response plan (or equivalent)
   - a public-facing privacy policy
   - internal guidance material, checklists and templates that inform how to manage privacy and respond to incidents
   - practices to consider the privacy impacts of any new projects and systems that involve personal information and undertake Privacy Impact Assessments when needed.

4. An indication of how the organisation will manage and govern the entity's DATA Scheme responsibilities and obligations.

Minimise the risk of unauthorised access, sharing or loss of data

The entity is able to minimise the risk of unauthorised access, sharing or loss of data (s77(1)(b) of the Act), evidenced by:

5. Identified role/s responsible for the organisation's security (Chief Security Officer or equivalent). This is including or in addition to the roles identified elsewhere in the application.
6. A governance body or bodies responsible for physical, ICT and data security governance.
7. Organisational policies and practices that document roles, responsibilities and processes for managing and governing physical, ICT and data security.

   These should demonstrate a risk-based approach to data security, be comparable to the guidance provided in the Protective Security Policy Framework (PSPF), and must include:

   - a Security policy or plan that covers data/ICT and identifies security risk owners, stewards or managers
   - a plan or process for security/incident reporting, investigation, monitoring or response
   - currency with recognised security standards
   - policies and procedures that address:
     - physical security controls
     - application controls for workstations and servers
     - vulnerability controls for applications and operating systems
     - application hardening controls for web and software applications
     - setting configuration controls for macros
     - administrative controls for account access
     - user and authentication controls
     - data security incident management

- ICT equipment management.

8. Controls for scheme data:
   - there is an approach to identifying scheme data, which may be Information Classification markings
   - scheme data containing personal information must be held in Australia
   - scheme data must be hosted by certified providers under the Digital Transformation Agency Hosting Certification Framework (or equivalent)
   - data backups and archives are held in Australia and are protected
   - cryptography arrangements must be in place for scheme data in transit and at rest.

This risk can also be addressed through the organisation nominating to:

- only store and manage data accessed through the DATA Scheme on a network that is rated Protected according to the Protected Security Policy Framework

OR

- only manage data accessed through the DATA Scheme using an Accredited Data Service Provider.

9. Workforce governance addresses personnel risks to data:
   - workforce vetting practices include identity and reference checks
   - staff in data roles who are based overseas can be identified
   - workforce offboarding measures include the revocation of access to data and systems where data is held.

Skills and capability

The entity has 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 (s 77(1)(c) of the Act), evidenced by:

10. Identified data specialist roles:
    - data analyst; and
    - data manager or data policy/governance.

    This is including or in addition to the roles identified elsewhere in the application.

11. Organisational policies and practices supporting data skills and capability show formal practices around data and include:
    - identified data analytics expertise, with common use of data analysis software packages to produce meaningful information
    - an established way of communicating about and describing data
    - ongoing support for staff data capability uplift
    - for staff who regularly interact with data, regular mandatory training that covers
      - data responsibility
      - security awareness
      - privacy.

12. Training for staff about the DATA Scheme.