



Australian Government



Inclusive
Employment
Australia

Inclusive Employment Australia Guidelines

Part A: Administrative Requirements

Disclaimer

These Guidelines are not a stand-alone document and do not contain the entirety of an Inclusive Employment Australia Provider's obligations. It must be read in conjunction with the Inclusive Employment Australia Deed 2025-2030 (the Deed), including any other relevant Guidelines and reference material issued by the Department of Social Services under or in connection with the Deed.

These Guidelines are not legal advice, and the Commonwealth accepts no liability for any action purportedly taken in reliance upon it and assumes no responsibility for the delivery of the Services. These Guidelines do not reduce the obligation of Providers to comply with their relevant legal obligations and, to the extent these Guidelines are inconsistent with obligations under the *Disability Services and Inclusion Act 2023* (Cth), Social Security Law, the *Privacy Act 1988* (Cth), Work Health and Safety (WHS) Laws or any other legislation or laws relevant to the respective jurisdictions in which Providers operate, the relevant legislation or laws will prevail.

Version History

Version 1.0 Published on: 17 July 2025

Effective from: 1 November 2025

Version 1.1 Published on: 21 November 2025

Effective from: 21 November 2025

In this version of the Guidelines, the visual identity has been updated to align with the Inclusive Employment Australia branding and the following Chapters have been updated:

- Chapter 1: Operational Requirement — includes new content on Inclusive Employment Australia branding
- Chapter 2: Provider Capability and Capacity – includes new content on mandatory training and claims for reimbursement under the Capacity Building Fund.



Contents

Guideline Interpretation and Glossary	7
Reading notes	7
Related information	7
Glossary	7
Chapter 1: Operational Requirements	9
1.1 Chapter Overview	9
1.2 Inclusive Employment Australia Branding	9
1.3 Minimum Site requirements	9
1.3.1 Co-location with other Providers or services	10
1.4 Recipient Created Tax Invoices	10
1.5 Fraud and Corruption responsibilities	10
1.5.1 Reporting Fraud or Corruption	11
1.6 Dispute Resolution	11
1.7 Media enquiries	12
Chapter 2: Provider Capability and Capacity	13
2.1 Chapter Overview	13
2.2 Caseload	13
2.3 Collaboration with other Providers and community organisations	13
2.3.1 National Disability Recruitment Coordinator	14
2.3.2 Australia’s Disability Strategy	14
2.4 Staffing requirements	14
2.4.1 Provider recruitment, training and development strategy	15
2.4.2 Staff qualifications and equivalent experience	15
2.4.3 Lived experience	15
2.5 Provider staff training	16
2.5.1 Mandatory training	16
2.5.2 Compliance with mandatory training requirements	18
2.6 Business continuity requirements	18
2.7 Capacity Building Fund	18
2.7.1 What is the Capacity Building Fund?	18
2.7.2 Eligibility for the Fund	19



2.7.3	Eligible Categories	19
2.7.4	Reimbursement of expenses	21
2.7.5	Lodging a Claim for Reimbursement.....	21
Chapter 3: Provider Servicing Standards		23
3.1	Chapter Overview	23
3.2	Code of Conduct and Service Guarantee	23
3.3	National Standards for Disability Services	24
3.3.1	Obtaining Certification	24
3.3.2	Maintaining Certification	25
3.4	Commonwealth Child Safety Framework	26
3.4.1	Resources for complying with the Child Safety requirements	26
3.4.2	Reporting of incidents	26
3.5	Customer Feedback Register	27
3.6	Complaint processes	27
3.6.1	Dealing with Participant Feedback and Complaints	27
3.6.2	Complaints Resolution and Referral Service	28
3.6.3	Department of Social Services Complaints	28
Chapter 4: Provider Performance Framework.....		30
4.1	Chapter Overview	30
4.2	Provider performance.....	30
4.2.1	Performance monitoring and assessment.....	30
4.2.2	Key Performance Indicators	30
4.2.3	Scoring performance.....	30
4.2.4	Release of Performance Scorecards	31
4.3	Performance Management.....	31
4.3.1	Provider Performance Monitoring	31
4.3.2	Compliance and Performance Improvement	32
4.3.3	Performance Improvement Plans	32
4.3.4	Performance Review and Business Reallocation	32
Chapter 5: Record Management Instructions		33
5.1	Chapter Overview	33
5.2	Records Framework	33



5.2.1	General Records Authority 40	34
5.3	Management of Records	34
5.3.1	Storage of Documentary Evidence in the Department’s IT Systems... ..	35
5.3.2	Storage Requirements.....	37
5.3.3	Control of Records	37
5.4	Movement of Records.....	38
5.5	Transfer of Records.....	38
5.5.1	Transfer between Providers	38
5.6	Data Migration	39
5.6.1	Data Security Considerations	39
5.6.2	Decommissioning of Systems.....	39
5.7	Breaches and Inappropriate Handling of Records	40
5.7.1	Reporting Requirements.....	40
5.7.2	Rectification Requirements	40
5.7.3	Notifiable Data Breaches	40
5.8	Retention of Records.....	40
5.9	Destruction of Records	41
5.9.1	Methods of destroying Records.....	42
5.9.2	General Records Authority 30	42
5.9.3	General Records Authority 31	43
Chapter 6:	Privacy.....	44
6.1	Chapter Overview	44
6.2	Where to find your obligations.....	44
6.2.1	Personal information and sensitive information.....	45
6.2.2	Consent and the APPs	45
6.3	APP 3 and 5: Collection of solicited personal information	46
6.3.1	Participant consent requirements	47
6.3.2	Consent to the collection of Sensitive Information	49
6.3.3	Manner of collection.....	51
6.4	APP 4: Dealing with unsolicited personal information.....	51
6.5	APP 6: Use and Disclosure of personal information.....	52
6.5.1	Information for ‘checks’	53
6.5.2	Information for ‘assessments’	53



6.5.3	Tax File Numbers	53
6.6	APP 7: Direct marketing	54
6.7	APP 9: Adoption, use or disclosure of government related identifiers	54
6.8	APPs 12 and 13: Access to and correction of personal information	54
6.8.1	Freedom of Information requests.....	55
6.9	Use and disclosure of Protected Information.....	56
6.9.1	Offences related to Protected Information.....	56
6.9.2	Permitted uses of Protected Information.....	56
6.9.3	Public Interest Certificates.....	57
6.10	Privacy Incidents and the Notifiable Data Breaches Scheme	57
6.11	Privacy Complaints	58
6.12	Referring individuals to the Department in relation to privacy matters...	58
6.13	Awareness and Training Expectations.....	58
6.13.1	Privacy Training Module	59
6.13.2	Staff Compliance	59
Chapter 7:	External Systems Assurance Framework.....	60
7.1	Chapter Overview.....	60
7.2	External Systems Assurance Framework.....	60
7.2.1	Providers' IT Systems	61
7.2.2	Third Party Employment Systems (TPES).....	61
7.3	Right Fit For Risk approach	62
7.4	Accreditation and maintenance of accreditation	62
7.5	Provider classification for accreditation.....	63
7.6	Milestones for completing the accreditation process	64
7.6.1	Milestone 1.....	64
7.6.2	Milestone 2.....	65
7.6.3	Milestone 3.....	66
7.7	Submission deliverables	67
7.7.1	Submission milestones.....	67
7.7.2	Deliverable descriptions	68
7.7.3	Considerations for accreditation commencement	70
7.7.4	Certifying Assessment Bodies	70
7.8	Accreditation maintenance.....	70



- 7.9 Core expectations of Providers under the RFFR..... 71
 - 7.9.1 RFFR Core Expectations: Personnel security 72
 - 7.9.2 RFFR Core Expectations: Physical security 73
 - 7.9.3 Essential Eight cyber security strategies 73
- 7.10 General requirements 74
 - 7.10.1 Security Contact..... 74
 - 7.10.2 Subcontractor and Third-Party IT Vendor requirements 74
 - 7.10.3 Access and information security assurance for External IT Systems .. 75
 - 7.10.4 Cloud Services Providers 75
 - 7.10.5 Request for extensions to meet RFFR accreditation requirements..... 75
 - 7.10.6 Breaches of security requirements under the Inclusive Employment Australia Deed 76






Guideline Interpretation and Glossary

Reading notes

These Guidelines, developed by the Department of Social Services (the Department), detail the objectives and operation of Inclusive Employment Australia.

The Guidelines may be updated or varied from time to time. The Department reserves the right to review and amend the Guidelines as deemed necessary and will provide reasonable Notice of any amendments.

The Guidelines use the following symbols to indicate different elements:

-  This icon represents 'System Steps' – information contained under this dot point will relate to usage of the Department's IT Systems.
-  This icon represents 'Work Health and Safety Steps' – information contained under this dot point will relate to matters of WHS Law.
-  This icon represents 'Documentary Evidence Requirement' – information contained under this dot point will relate to matters of Documentary Evidence.

Related information

Reference information and websites relevant to these Guidelines include:

- [Disability Services and Inclusion Act 2023](#)
- [National Standards for Disability Services](#)
- [Freedom of Information Act 1982](#)
- [Privacy Act 1988 \(Cth\)](#)
- [Archives Act 1983](#)

Glossary

All capitalised terms in these Guidelines have the same meaning as in the Deed unless otherwise defined below.

Breach is a failure by a Provider to meet or perform their obligations under the Deed.

Caseload means, in relation to the Provider at a particular point in time, all Participants who have on or before that point in time been Referred to, or Directly Registered with, the Provider and have not been Exited or transferred to another Inclusive Employment Australia Provider since that Referral or Direct Registration.

Inclusive Employment Australia Payment Assurance Program or **Inclusive Employment Australia-PAP** is a quarterly review of Documentary Evidence and/or third-party verification for a random selection of claims.

Inclusive Employment Australia Provider has the same meaning as Program Provider in the Deed.

National Disability Recruitment Coordinator or **NDRC** means the JobAccess program of that name, administered by the Department.

National Standards for Disability Services Audits or **NSDS Audits** are independent audits of Providers conformance with the National Standards for Disability Services (NSDS). Audit reports are provided to the Department and used to monitor Provider compliance and quality of service.

Performance Rating means a rating (Exceeds, Meets, or Improvement Required) issued to Providers in the Performance Scorecards after the Department has assessed them against each KPI.



Performance Scorecard means a high-level summary of the Provider's performance published by the Department for the information of Participants and other stakeholders.

Privacy Law means the *Privacy Act 1988* (Cth) and the Australian Privacy Principles.

Performance Improvement Plan or **PIP** is a Provider-developed strategic plan to improve performance against the Key Performance Indicators for the Inclusive Employment Australia Performance Framework.

Service Recipient means someone who is receiving or is in the process of applying for a social security payment, benefit, or allowance.



Chapter 1: Operational Requirements

[Supporting Documents](#) for this Chapter

- Joint Charter for Disability Employment Programs and Related Services
- [Inclusive Employment Australia Brand Guidelines](#)
- [Commonwealth Fraud and Corruption Control Framework 2024](#)

1.1 Chapter Overview

The following Chapter outlines various operational requirements for Providers in delivering Services under their Deed.

1.2 Inclusive Employment Australia Branding

The Inclusive Employment Australia brand has been developed to identify and support disability open employment services delivered by the Australian Government.

Providers must use the Inclusive Employment Australia brand in the delivery of Services and in accordance with the [Inclusive Employment Australia Brand Guidelines](#). The Brand Style Guide is a Guideline for the purposes of the Inclusive Employment Australia Deed.

1.3 Minimum Site requirements

Providers must ensure their Sites (including operating from local libraries, town halls or other similar venues) meet the following minimum requirements:

- Be presented in a manner that upholds and maintains the good reputation of the Services, the Department and Inclusive Employment Australia, as determined by the Department
- Be accessible to people with disability consistent with universal design principles. This includes making available disability parking spaces (accessible parking) and accessible toilet facilities
- Make available job search facilities for Participants to assist with Résumé writing, job applications and interview preparation. The Service Guarantee requires providers to help Participants with services and supports including job search support, accessing non-vocational programs and further education or training. It is reasonable to expect providers make appropriate job search facilities available for Participant use, including computers with internet access and printers
- Be compliant with the National Standards for Disability Services (NSDS)
- Display the required Inclusive Employment Australia signage, including information for Participants about the Service Guarantee and Code of Conduct
- Ensure materials provided, shared, used, and displayed are accessible to all Participants
- Protect participant privacy. This must be a safe, private environment. Participants confidentiality must be assured as discussions can often include conversations about complex barriers. Participants may share sensitive information. Facilities and protocols must be in place to ensure security of Personal Information and a Participant's privacy, and
- Be inclusive and culturally safe to cater to the needs of participants so that Services can be delivered in a safe manner, compliant with Work Health and Safety Laws.



Providers are not to meet a participant at the participant's home or place of residence.

It is a Provider's responsibility to obtain approval/permission from the relevant site owner to deliver Inclusive Employment Australia Services from the Site (including libraries, town halls, community spaces or other venues). A Provider must be able to provide this proof of approval to the Department if the Department requests it.

1.3.1 Co-location with other Providers or services

The Department considers a Site to be co-located where one or more Providers, employment service program, or third-party organisation is interacting with Participants. This is a single Site including any shared space, reception, waiting areas, service areas and meeting rooms.

In addition to the minimum general requirements for a Site stated above, where multiple Providers, employment services, and/or third-party organisations are co-located at a single Site, the Department requires Providers to:

- assist Participants visiting the Site with clear advice about the Services delivered at the Site
- provide each Participant with accessible information about the Site, Provider and employment service to which they have been Referred
- present signage in accordance with Section 1.2 Inclusive Employment Australia Branding. This includes identifying the broader workspace with the Services being delivered to help Participants understand where they need to go, and identifying staff members' roles to help Participants understand who they should talk to, and
- have clear protocols and accountabilities established about the use of shared space and facilities (for example, use of printers, copiers, private rooms and storage).

1.4 Recipient Created Tax Invoices

The Department may issue a Tax Invoice to the Provider in relation to Payments made by the Department to the Provider for the delivery of Services under the Deed. This Tax Invoice will be a recipient created Tax Invoice (RCTI) for the purposes of the *Goods and Services Tax (GST) Act 1999* and will be labelled as an RCTI when issued by the Department. The Provider is not required under the Deed to submit a Tax Invoice to the Department when this occurs. The Department is registered for GST and will notify the Provider if it ceases to be registered for GST.

1.5 Fraud and Corruption responsibilities

Providers should be aware of Fraud and Corruption risks that exist within the delivery of employment Services. Providers must put in place Fraud and Corruption detection practices, policies and procedures, that are reviewed annually. Procedures should include a clear reporting process for suspected Fraud or Corruption.

Providers must ensure its staff, Subcontractors and agents comply with and take all reasonable steps to enable the Commonwealth to comply with the Commonwealth Fraud Control Framework (Framework). The Framework is available at [Commonwealth Fraud and Corruption Control Framework 2024](#).

The Provider must take all reasonable steps to prevent, mitigate and detect Fraud and Corruption in accordance with the Framework. This includes implementing a Fraud and



Corruption Control Plan and conducting a Fraud and Corruption Risk Assessment. A copy of the plan must be provided to the Department on request.

Providers must ensure all staff who deliver Services under the Deed complete the Fraud and Corruption training module when they commence with the Provider or Service and complete this training annually.

1.5.1 Reporting Fraud or Corruption

Current and former staff of a Provider and contractors must report suspected fraud or corruption to the Department's fraud team via fraud@dss.gov.au or DSS Fraud Hotline on 1800 054 312. They must encourage others who are outside the contractual arrangement such as Participants or members of the public to report any suspected fraud or corruption.

When reporting Fraud or Corruption, the person reporting should provide as much information as possible, for example:

- **Who** is the subject of the suspected Fraud or Corruption?
- **When** and **where** did the suspected Fraud or Corruption occur?
- **What** sensitivities, if any, there may be?
- **How** did the subject/s commit the suspected Fraud or Corruption?

If there is any information available that supports the allegation, this information should also be provided.

(Deed reference(s): clause 31)

Suspected serious or systemic corruption by or involving current or former Provider staff can be reported directly to the National Anti-Corruption Commission (NACC) — see the NACC's website [How to make a report](#). A range of protections are available to those who report directly to the commission.

1.6 Dispute Resolution

Providers are expected to work with the Department to resolve complaints, disputes or problems, using the following resolution process (except for matters excluded under the Deed):

- Any dispute arising in relation to the Deed will be dealt with, in the first instance, through the informal process set out in the Joint Charter for Disability Employment Programs and Related Services issued by the Department
- If any dispute arising in relation to the Deed cannot be resolved using the informal process, the following will occur:
 - the Party claiming a dispute will provide the other Party a written Notice that sets out the nature of the dispute
 - within 5 Business Days of receipt of the Notice, each Party will nominate a representative from the entities who have not been previously involved in the dispute, and
 - the Parties' representatives will try to settle the dispute by direct negotiation.
- If the dispute is not resolved within 10 Business Days after the date that the direct negotiation occurred, the Party claiming there is a dispute will refer the dispute to an independent third person. This person must be agreed between the Parties, and will have power to mediate and recommend a non-binding resolution.



- If the dispute is not resolved within 10 Business Days after the date that the dispute was referred to an independent third person, the Party claiming a dispute will refer the dispute to another independent third person. This person must be agreed between the Parties, and will have power to intervene and direct a resolution that the Parties will be bound by.
- If agreement on an independent third person cannot be reached or the dispute is not resolved within 20 Business Days after referring the dispute to an independent third person, either Party may commence legal proceedings.

Each Party will be responsible for its own costs arising from dispute resolution. Where an independent third person engaged the cost will be split equally between both parties.

(Deed reference(s): Clause 65)

1.7 Media enquiries

Engagement with the media can be an important part of the role of Providers.

Providers must immediately refer any media enquiries related to Government policy or program settings to the Department's media team (media@dss.gov.au) and their Account Manager. The email should include the nature and timeframe of the request and any relevant background.

The Department's media team will prepare and manage media responses.

Providers must immediately inform their Account Manager of any media enquiries received related to delivery of the Inclusive Employment Australia. The Account Manager will then advise if the media enquiry must be referred to the Department's media team.



Chapter 2: Provider Capability and Capacity

2.1 Chapter Overview

Paid employment supports people with disability to have more control over their lives, be financially independent and have a better standard of living. Employment also leads to better mental and physical health and wellbeing. Increasing employment opportunities for people with disability includes encouraging business ownership and development, self-employment and entrepreneurship.

To achieve the above, this Chapter outlines the desired capabilities and capacity of Providers to deliver tailored Services to both Participants and Employers, as well as supports available to Providers.

2.2 Caseload

Inclusive Employment Australia is demand-driven which means there is no cap on the total number of people who can participate in the service.

Providers are allocated a Caseload, subject to the Market Share threshold or the maximum number of Participants for a Site.

2.3 Collaboration with other Providers and community organisations

Providers will leverage local connections to deliver tailored Services to Participants. Providers are expected to build strong relationships with Employers to build their confidence and capability to attract and employ people with disability, injury or health condition.

In delivering Services for Participants and Employers, Providers are expected to identify and collaborate with disability, health, training and other community organisations and local (or regional) resources who support Participants in becoming work ready and creating Employment pathways. This includes, but is not limited to, engaging with:

- the National Disability Recruitment Coordinator (NDRC)
- other Inclusive Employment Australia Providers
- other Employment Services providers
- Employer stakeholders, such as local business councils
- private and community-based providers of other services in the community
- Education and Training institutions
- healthcare organisations
- social enterprises
- Aboriginal Community Controlled Organisations
- National Disability Insurance Scheme (NDIS) Local Area Coordinators, Support Coordinators and employment service providers
- Supported Employment Services (previously known as Australian Disability Enterprises)
- Other Commonwealth, State and Territory Government program providers



- local government and local government program providers, and
- peak bodies and industry representatives.

Providers should draw on these relationships in the locations they service to:

- support access to disability inclusive, culturally appropriate, linked Complementary Services for Participants
- maintain strong labour market knowledge, including knowledge of skill shortages
- develop and adapt activities to meet the diverse needs of businesses and industries, and
- create Employment pathways for Participants.

(Deed Reference(s): Clause 8)

2.3.1 National Disability Recruitment Coordinator

Providers must be aware of the National Disability Recruitment Coordinator (NDRC). The NDRC works with Employers to increase their recruitment of people with disability. It helps the Employer implement practices to employ people with disability, train staff in working with employees with disability and support recruitment of people with disability by the Employer.

Providers can:

- [Register for Updates](#) to learn about vacancies from employers looking for candidates with disability and get the JobAccess newsletter
- help Participants apply for roles
- go to events hosted by the NDRC – check News for the latest event invitations or sign up for the JobAccess newsletter
- refer Employers who might benefit from 12-month partnership with the NDRC

For more information about connecting with a NDRC visit the [JobAccess website](#).

(Deed Reference(s): 124)

2.3.2 Australia's Disability Strategy

Employment and financial security are central to improving outcomes for people with disability. This includes providing jobs and career opportunities and having adequate income for people to meet their needs. The Strategy and its supporting documents assist Providers with practical tools including:

- [Good Practice Guidelines for Engaging with People with Disability](#)
- [Guide to Applying Australia's Disability Strategy 2021-2031](#)
- [Evaluation Good Practice Guide Checklist](#).

For more information about Australia's Disability Strategy visit the [Disability Gateway](#).

2.4 Staffing requirements

Providers will continuously invest in leadership and front-line staff and will demonstrate they have the appropriate skills, qualifications, experience and diversity that is reflective of the communities and the Participants they support.



2.4.1 Provider recruitment, training and development strategy

Staff skills, experience and qualifications are considered a major contributor to the quality of services in employment services. Increasing the knowledge, experience and qualifications of Provider staff is key to lifting the quality of employment services and outcomes for people with disability.

When requested by the Department, Providers must provide a documented strategy that outlines their plan for staff recruitment, training, development and retention. It should detail how they will support professional development for their staff including dedicated learning and development, arranging specialist and mandatory training and pathways for staff to gain further qualifications.

The strategy must also include performance metrics which are required to be provided to the Department at regular intervals (at least annually) over the course of the Deed on the qualification and experience of staff and leadership, including, staff:

- with qualifications
- who are working towards obtaining qualifications, including micro-credentials
- who have disability
- who have a lived experience of disability, and
- who reflect broader diversity in their community.

Over the course of the contract period, Providers may be required by the Department to provide evidence that they are actively supporting the professional development of its staff.

(Deed Reference(s): 74)

2.4.2 Staff qualifications and equivalent experience

While accredited qualifications are not mandatory for Provider staff, it is expected Provider staff who are delivering Services to Participants and Employers either hold or be working towards one or more of the following credentials:

- a Certificate IV in Employment Services
- Certificate III or higher in Disability Services, or related qualifications
- units or micro-credentials within a related qualification, or
- professional learning modules for employment service professionals.

They may also have relevant related experience to support them in their role, such as:

- lived experience
- relevant work experience, for example working with people with disability, or
- industry experience relevant to the local labour market.

(Deed Reference(s): 74.2)

2.4.3 Lived experience

Providers are encouraged to engage staff with disability or lived experience of disability as part of their staff recruitment, training and development approach over the life of the Deed. Lived experience is the experience of a person with disability. It may include the experience of a person who supports or cares for a person with disability, or a person



who has worked with and/or supervised a person with disability and understands reasonable adjustments (work adjustments) that enable people with disability equal access to employment.

2.5 Provider staff training

2.5.1 Mandatory training

Provider staff must undertake mandatory training developed by the Department. Provider staff cannot perform some functions until they have completed the relevant training module.

Training module	Restriction if incomplete
Privacy	Cannot access Workforce Australia Online for Providers.
Fraud and Corruption	Cannot access Workforce Australia Online for Providers.
Targeted Compliance Framework	Cannot access Compliance actions (includes booking re-engagement appointments).
Job Plans	Cannot create, update or remove Job Plans (includes booking initial appointments).
Claims Processing – Outcome Fees	Cannot claim payments (includes Outcome payments, Progress payments, Wage subsidies and request payments).
Claims Processing – Progress Fees	Cannot claim payments (includes Outcome payments, Progress payments, Wage subsidies and request payments).
Claims Processing – Wage Subsidies	Cannot claim payments (includes Outcome payments, Progress payments, Wage subsidies and request payments).
National Panel of Assessors – Ongoing Support Assessments	Cannot conduct Ongoing Support assessments.
Supported Wage System	Cannot complete Supported Wage System assessments.

All mandatory training can be found on the Learning Centre platform. Providers must ensure all mandatory training modules are completed by Provider staff according to the timeframes below.

Other training modules are also available, covering essential information for Providers and their staff to understand Inclusive Employment Australia, as well as content on supporting people with disability, disability awareness and cultural competency.

As part of staff onboarding

Providers must notify staff and ensure they are aware the Department will collect, use and disclose Personal Information about Provider staff for the purposes of managing and administering Inclusive Employment Australia. This may be in the form of a Privacy Collection Notice and/or consent form and must include matters as required by APP 5.2.



This collection notice may include (but is not limited to):

- disclosing Personal Information of Provider staff (including the names and contact details of Organisational Security Contacts), to enable the Department to support the ICT system used for Inclusive Employment Australia
- disclosing Personal Information of Provider staff if required to report particular conduct (e.g. serious incidents)
- using and disclosing Personal Information of Provider staff in relation to complaint handling
- disclosing Personal Information of Provider staff in relation to the management of Inclusive Employment Australia to DEWR, the Department, Employers, NPA Providers, the CRRS, JobAccess Providers, and any other third-party organisations
- collecting sensitive information in particular circumstances (e.g. in delivering culturally appropriate services because they identify as Aboriginal and/or Torres Strait Islander)
- authenticating the Provider staff's access to the ICT system, and subsequently logging and monitoring all activity on the system, to make sure it is being used appropriately, and
- ensuring that the Provider is complying with its obligations under the Inclusive Employment Australia Deed.

The following modules must be completed by each staff member before being granted access to the Department's IT Systems:

- Fraud and Corruption, and
- Information Exchange and Privacy.

These two mandatory training modules must be refreshed every 12 months to maintain compliance.

Provider staff must also acknowledge their security and privacy obligations in relation to the use of the IT system and access to participant information.

Prior to Participant engagement

Before delivering Services to Participants, each staff member must complete the following module:

- Job Plans, and
- Targeted Compliance Framework.

Additional Mandatory Training

Within 60 days of starting to deliver Services for Inclusive Employment Australia, or from the date the training is first available, each staff member will need to complete any other modules flagged as mandatory on the Learning Centre platform. The Department will notify Providers of new training requirements for their staff.

(Deed Reference(s): 61.3)

To submit claims for Payment

Provider staff who submit claims for payment must complete Claims Processing Training Modules prior to making any claim.

(Deed Reference(s): 157.4)



2.5.2 Compliance with mandatory training requirements

Providers must monitor and annually self-audit staff completion of mandatory training and report to the Department. The Department may request details of a Provider's self-audit at any time and may conduct its own audit of a Provider's compliance with mandatory training requirements, where this may be deemed necessary.

2.6 Business continuity requirements

From time to time the Department or Commonwealth may temporarily close a Site due to national emergency management.

Providers are required to have business continuity plans established to ensure provision of employment services to Participants is provided during emergencies or other incidents leading to business disruption, where it is safe to do so.

At a minimum, arrangements should include processes to:

- contact affected Participants, if required
- ensure that Targeted Compliance Framework (TCF) is not applied where Mutual Obligation Requirements have been Suspended
- arrange alternative servicing options for Participants, if appropriate
- reschedule Appointments or Activities, including contacting Employers, host organisations, or support services
- manage Site safety and security, including lockdowns or evacuations
- manage the security and integrity of Provider IT Systems, including containment and notification to the Department of cyber incidents
- secure Records and filing systems, and
- submit urgent/critical notifications and incident Reports (including temporary Site closure Reports) to the Department and other relevant entities (e.g. police, health/welfare agencies, emergency respondents).

More information on [Disability Inclusive Emergency Management](#) is available on the NEMA website.

2.7 Capacity Building Fund

2.7.1 What is the Capacity Building Fund?

The Capacity Building Fund (the Fund) was introduced to assist eligible Providers establish themselves and build their organisational capability under the Inclusive Employment Australia program.

The Fund may be accessed by Providers that meet the eligibility criteria by submitting a Claim for Reimbursement form (with relevant documentary evidence and latest audited financial statements) in respect of Eligible Expenditure.

Once a claim for reimbursement is approved by the Department, payment will be made to the Provider's nominated bank account on a reimbursement basis in the amount(s) approved by the Department. The Department has absolute discretion over the decision to approve the reimbursement.



This Chapter sets out Provider eligibility for the Fund and provides guidance around the categories of costs that can be reimbursed under the Fund and how claims for reimbursement can be submitted.

2.7.2 Eligibility for the Fund

For an Inclusive Employment Australia Provider to be eligible for the Fund, the following criteria, which is set out at clause 167.1 of the Deed, must be met:

- the Department has executed a Deed with the Provider, and
- the Provider meets the definition of a 'Small Business' under the Deed, and
- the Provider is either:
 - a not-for-profit organisation, or
 - a Specific Cohort Provider under Inclusive Employment Australia.

Subcontractors are not eligible for the Fund.

Small Business

The Provider must be a Small Business as defined at clause 167.6 (c) of the Deed.

Eligibility as a Small Business is based on the Provider's most recent financial statements at the time the Deed is executed.

Where the Provider tendered as a Group, all members of the Group, including the lead member, will be assessed in aggregate to determine if the Provider is considered a Small Business.

Not for Profit Organisations

To be eligible for the Fund as a not-for-profit organisation, the Provider must be listed on the Australian Charities and Not-for-profits Commission's register of registered charities found at [Recently registered charities](#).

Specific Cohort Providers

To determine eligibility for the Fund, the Department will refer to the Provider's executed Deed to confirm they deliver Services as a Specific Cohort Provider.

A Group Respondent that includes specialist organisations will only be eligible if the Group Respondent is a Specific Cohort Provider.

2.7.3 Eligible Categories

Eligible Expenditure for reimbursement categories are:

- achieving compliance with the NSDS
- obtaining Right Fit For Risk (RFFR) accreditation
- building organisational leadership
- supporting mentorship arrangements for Provider Personnel
- supporting effective service delivery
- business advisory and management consulting services
- financial planning and accounting services
- acquiring and maintaining essential ICT equipment



- training for Provider Personnel and other relevant training and development services, and
- any other accreditation, certification or professional capability or capacity specified in the Guidelines.

Reimbursements are only payable for expenses that are incurred by the Provider on or after the date the Deed has been executed by the Parties (the Provider and Department). For example, if a Provider has commenced obtaining quality certification before the Deed has been executed, only those expenses incurred on or after the date the Deed was executed are reimbursable.

Providers cannot seek Reimbursement for the same expenses that have already been reimbursed or paid for by another Commonwealth Agency.

The Department will not fully prescribe every type of expenditure that may be covered in each category. The general principle is the costs or expenses must relate directly to delivering the Inclusive Employment Australia program. The following examples are provided as guidance.

National Standards for Disability Services (NSDS) Certificate of Compliance

The Fund may be used for reimbursement relating to costs and expenses associated with the Provider obtaining and maintaining NSDS certification required to deliver the Inclusive Employment Australia program.

A Provider is considered certified against the NSDS when they have received certification from a third-party auditor approved by the Department. Once this certification is attained by the Provider, a claim for reimbursement under the Fund can be made. Providers may seek reimbursement for initial certification, surveillance audits or re-certification NSDS audits. More information on NSDS listed at section 3.3 of the National Standards for Disability Services.

Right Fit for Risk (RFFR) Accreditation

Claims for reimbursement related to RFFR Accreditation may include:

- expenses relating to the design and implementation of a system to meet relevant information security requirements
- software upgrades, new hardware or other IT infrastructure to comply with information security requirements
- purchase of ICT equipment required to meet cyber security accreditation requirements
- hiring additional staff specifically to obtain certification/accreditation, and
- engaging a third party/IT company to assist with the accreditation process.

More information about RFFR can be found at 7.3 Right Fit For Risk approach.

Training for Provider Personnel

Reimbursable costs and expenses for training and development of Provider Personnel may include:

- the attainment of relevant accredited tertiary, Diploma or Certificate III or IV level qualifications
- training courses relating to the delivery of disability employment services or supporting people with disability.



Note: Any courses reimbursed under the Fund for this purpose must not be delivered directly by the Provider or by a Related Entity of the Provider.

2.7.4 Reimbursement of expenses

Reimbursements under the Fund are capped at \$150,000 (GST inclusive) per Provider, for the life of the Deed Term (including any Deed extensions). All expenses submitted for reimbursement must be **GST inclusive**.

Reimbursements are payable for any expenses or costs incurred after the Inclusive Employment Australia Deed was executed on 7 August 2025.

For Group Respondents, reimbursements can be claimed for Eligible Expenditure by any group member so long as the Group as a whole meets the criteria at 2.7.2 above.

2.7.5 Lodging a Claim for Reimbursement

All claims for reimbursement must be lodged within 30 days of payment for the goods or services.

To claim, Providers must complete the Claim for Reimbursement form available on the Provider Portal and email it together with all required Documentary Evidence to CBFPayments@dss.gov.au for assessment.

The table below outlines Documentary Evidence required when seeking reimbursement for Eligible Expenditure.

Eligible Expenditure	Documentary Evidence / process
Financial support to achieve NSDS compliance and RFFR accreditation	<ul style="list-style-type: none"> • An email from DEWR advising RFFR accreditation has been achieved • NSDS Certificate of Compliance • Valid Tax Invoice demonstrating audit costs related to attaining RFFR accreditation • Timesheets for staff wages that relate to attaining RFFR accreditation • Evidence of payment from the Provider to a third-party supplier, such as: <ul style="list-style-type: none"> ○ a record of transaction (bank statement or a record of transaction from the organisation’s financial system) ○ a Tax Invoice with the receipt from the supplier ○ a remittance advice, or ○ other valid proof of payment.
All other eligible categories	<ul style="list-style-type: none"> • Valid Tax Invoice and receipt • Evidence of payment for equipment purchased • Staff timesheets demonstrating time spent on training • A contract or other document that sets out mentorship arrangements, and • Examples of training and development opportunities provided to staff.



2.7.6 Assessment of Reimbursement

The Department will consider each claim for reimbursement and email the Provider of its decision. The Department has absolute discretion regarding its decision to approve the claim for reimbursement.



Chapter 3: Provider Servicing Standards

[Supporting Documents](#) for this Chapter

- [Disability Services and Inclusion Act \(Cth\) Code of Conduct](#)
- [National Standards for Disability Services](#)
- [Disability Services and Inclusion \(Compliance Standards and Alternative Compliance Requirements\) Rules 2023](#)
- Inclusive Employment Australia Audit Scheme
- [National Standards for Disability Services – Self Assessment Worksheets](#)
- Inclusive Employment Australia Service Guarantee
- Accredited certification bodies for Inclusive Employment Australia
- [Department of Social Services Complaints Form](#)

3.1 Chapter Overview

This Chapter outlines various standards Providers are required to adhere to in delivering Services under their Deed.

3.2 Code of Conduct and Service Guarantee

The [Code of Conduct](#) under the *Disability Services and Inclusion Act 2023* (Cth) and the [Service Guarantee](#) aim to ensure each Participant receives a high-quality service.

The requirements of the Code of Conduct are core expectations about Provider practices for all disability support and services.

As the service is legislated through the *Disability Services and Inclusion Act 2023* (Cth), Providers are required under the Code of Conduct to:

- act with respect for the individual rights of people with disability to freedom of expression, self-determination and decision making, following applicable laws and conventions
- respect the privacy of people with disability
- provide Services in a safe and competent manner, with care and skill
- act with integrity, honesty and transparency
- promptly take steps to raise and act on concerns about matters that may change the quality and safety of the provision of the activity to people with disability
- take all reasonable steps to prevent and respond to all forms of violence, exploitation, neglect and abuse of people with disability, and
- take all reasonable steps to prevent and respond to sexual misconduct.

Providers must prominently display Code of Conduct and Service Guarantee promotional Material in each of its offices and on its website at all times.

Non-compliance with the Code of Conduct will constitute a Breach of the Deed which may result in the Department taking remedial action against the Provider, which could include suspension of Payments or Referrals, or termination of the Deed.

The Service Guarantee specifies the minimum Services each Participant can expect to receive from their Provider.

(Deed Reference(s): Clause 110 and 111)



3.3 National Standards for Disability Services

The [National Standards for Disability Services](#) (NSDS) promote and drive a nationally consistent approach to improving the quality of services. They focus on rights and outcomes for people with disability.

The NSDS, outlined in the [Disability and Inclusion \(Compliance Standards and Alternative Compliance Requirements\) Rules 2023](#), are the compliance standards for regulated activities under the *Disability Services and Inclusion Act 2023* (Cth).

Inclusive Employment Australia is considered a regulated activity of the *Disability Services and Inclusion Act 2023* (Cth). Organisations receiving Funding under this deed must obtain and maintain a Certificate of Compliance against the NSDS.

Inclusive Employment Australia Providers must be certified against all 6 standards in the NSDS for the first accreditation audit in a 3-year cycle. This 3-year cycle is supported by annual surveillance audits conducted within 12 and 24 months of receiving accreditation.

Eligible Providers can access funding through the Capacity Building Fund to help with the cost of the audits. More information about this funding can be found at Chapter 2:

Provider Capability and Capacity.

3.3.1 Obtaining Certification

To obtain a Certificate of Compliance, Providers will have an audit undertaken with an accredited certification body. Audit requirements will be detailed in the [Inclusive Employment Australia Audit Scheme](#) document. The Scheme outlines how certification bodies undertake audits and the timeframes for first audit and reviews.

Certification bodies are accredited by the Joint Accreditation System of Australia and New Zealand (JASANZ).

Audit Process

Step by step process for initial audit to obtain a Certificate of Compliance:

- **Step 1. Start the process**

Prepare for your audit by reviewing your organisation's structure, policy and procedures following your contractual requirements.

Resource: [National Standards for Disability Services – Self Assessment Worksheets](#).

- **Step 2. Choose a certifying body**

Select a certification body and negotiate a contract for them to conduct your audit. Liaise with them to arrange the start of your organisation's auditing activities.

Resource: The [Accredited certification bodies for Inclusive Employment Australia](#) document available on the Provider Portal.

- **Step 3. Planning your certification audit**

Provide your auditor with your organisation's policies and procedures as requested to help a stage 1 audit. Discuss any logistical needs for your on-site stage 2 audit.

Resource: [Supporting Documents for NSDS](#).



- **Step 4. Prepare for your on-site certification audit**

Liaise with certification body about on-site audit activities, including sampling. Negotiate on-site visit dates and prepare Participant involvement in audit, including obtaining consent.

- **Step 5. Follow up actions**

If identified, address nonconformities (NCs) within the required timeframes. Major NCs must be resolved within 3 months and minor NCs within 6 months of the audit assessment.

The decision on certification must be made no later than 15 months after the date the Determination is signed. Certification cannot be issued whilst there are unresolved NCs.

Provide feedback to staff, Board and Participants to facilitate continuous improvement.

- **Step 6. Receive Certificate of Compliance**

After your on-site certification audit, the auditing team will provide your organisation with a draft written report for your review. The final report and certification decision must be provided to your organisation and the Department.

If the decision is to certify, then your Certifying Body will issue your organisation a Certificate of Compliance, which is valid for 3 years.

- **Step 7. Send Certificate of Compliance**

Once you receive your Certificate of Compliance send a copy to the Department along with your final audit report.

3.3.2 Maintaining Certification

The Provider organisation must take part in a surveillance audit to keep their accreditation under the NSDS. A full re-certification audit must be completed within 36 months of the first certification date.

Annual surveillance audits (surveillance 1 and surveillance 2) are conducted against NSDS standards 1, 3 and 6 and at least one other standard that is chosen by an accredited certifying body. Provider organisations must take part in surveillance audits to maintain their certification against the NSDS.

Providers should follow this step-by-step process during the 3-year certification cycle in order to maintain certification:

- **Step 1. Undertake surveillance 1 audit**

- Undertake surveillance 1 audit within 12 months of the last day of the on-site component of the certification audit
- Address any NCs identified in the audit, and
- Send a final copy of the Report to the Department.

- **Step 2. Undertake surveillance 2 audit**

- Undertake surveillance 2 audit within 24 months of the certification audit, and within 12 months of the last day of the on-site component of the surveillance 1 audit



- Address any NCs identified in the audit, and
- Send a final copy of the Report to the Department.
- **Step 3. Undertake recertification audit**
 - Address any NCs identified in the audit
 - Finalise recertification, including resolving any NCs, before the current Certificate of Compliance expires, and
 - Send a final copy of the Report and new Certificate of Compliance to the Department.

(Deed Reference(s): Clause 98.3)

3.4 Commonwealth Child Safety Framework

In response to the Royal Commission into Institutional Responses to Child Sexual Abuse, the Australian Government developed the Commonwealth Child Safe Framework (CCSF) policy that sets out the minimum standards for Child safe practices within Commonwealth entities. The Commonwealth response includes a commitment to require any institution it funds to undertake Child-related work to adopt the National Principles for Child Safe Organisations ([National Principles](#)).

Where the CCSF is relevant, the Department has included Child Safety clauses into Deed. As specified in the Deed, Providers must undertake a range of actions to ensure child-safe standards and practices are available and implemented. Amongst other things, Providers must follow applicable Working with Children Laws, obtain Working with Children Checks where needed, and implement the National Principles (including to undertake a risk assessment, provide training and ensure compliance).

Providers must certify compliance annually with the Child Safety clauses. The Department will provide a Child Safety Provider Declaration each year, which Providers must complete and return by 31 March of that year.

3.4.1 Resources for complying with the Child Safety requirements

While the Department acknowledges that child safety-related laws differ between the States and Territories, Providers operating in multiple jurisdictions are responsible for ensuring they comply with those laws and have processes and policies in place complying with those laws and their Personnel are aware of their obligations under those laws.

Providers can refer to the Australian Human Rights Commission's (AHRC) [Child Safe Organisations website](#) for a list of state and territory child safety links, practical tools and resources to help implement the [National Principles for Child Safe Organisations](#), including free e-learning modules developed by the AHRC to help in training Provider Child-Related Personnel. Resources are also available from State and Territory governments in relation to compliance with Working with Children Laws.

3.4.2 Reporting of incidents

While delivering Services, Providers may identify concerns they have about a Child or Children, whether they are a Participant or not. Providers must ensure these concerns are actively and appropriately managed in line with their policies and procedures, the



National Principles and relevant legislation in the State and Territory jurisdictions they operate in, including those requirements relating to mandatory reporting in those jurisdictions.

Providers must notify the Department if there are any failures to comply with the Child Safety Obligations along with any actions taken to manage impacts to the Child(ren).

(Deed Reference: 22)

3.5 Customer Feedback Register

Providers must set up, and publicise to Participants, the existence and details of a feedback process about its performance and Services, including Complaints.

Providers must keep a Customer Feedback Register which includes, at a minimum, the following information:

- Customer Name
- Customer DOB
- Customer Contact Details
- Date of Feedback
- Time of Feedback
- Brief Summary of Feedback, and
- Actions Taken, if any.

(Deed Reference(s): 36-38)

3.6 Complaint processes

3.6.1 Dealing with Participant Feedback and Complaints

Providers must have internal policies and processes to manage Participant feedback and Complaints. Feedback and complaint resolution should be managed at the provider level in the first instance. Providers must:

- explain feedback and complaint processes to Participants on initial Contact, including potential Participants upon first Referral to, or on Direct Registration with, the Provider and to Participants at any time upon request
- ensure copies of feedback and complaints policies and processes are made available to Participants or other relevant users upon request
- ensure all feedback and complaints received are investigated appropriately by a senior staff member
- ensure all other feedback received is dealt with appropriately and positive feedback is also provided to relevant employees
- effectively communicate to the Participant that their complaint may be referred as necessary to either the Provider, the Department or the CRRS for investigation
- effectively communicate the outcome and actions of any investigation to the complainant and, if requested by the Department, to relevant entities such as the Customer Resolution and Referral Service (CRRS)
- assess whether a complaint relates to the Code of Conduct and, if it does, promptly inform the Department of the Complaint



- refer a Participant who is dissatisfied with feedback or complaint resolution to the CRRS in the first instance – 1800 880 052, and
- refer a Participant who would like to transfer to a different Provider to the National Customer Service Line (NCSL).

3.6.2 Complaints Resolution and Referral Service

The Complaints Resolution and Referral Service (CRRS) is an independent service funded by the Department to provide an independent, fair, impartial, and nationally accessible complaints resolution and referral service for people with disability who use Inclusive Employment Australia or Advocacy Services. This is funded through the *Disability Services and Inclusion Act 2023* (Cth). Providers must actively help the CRRS to resolve complaints reported to the CRRS. The CRRS is focused on local level resolution and will contact Sites in the first instance to ensure feedback and complaints are rectified at the source.

When engaged by the CRRS, Providers must:

- actively help in its investigation of the matter
- engage in negotiating a resolution including, where needed with other authorities, if the relevant Participant has chosen to utilise other legislative or administrative complaints mechanisms
- not withhold Services from a Participant who provides feedback or makes a complaint, or discriminate against a Participant because of feedback or a complaint, and
- record CRRS recommendations for service improvements and implement relevant recommendations or otherwise provide reasons to CRRS or the Department why the recommendations have not been implemented.

3.6.3 Department of Social Services Complaints

If a Participant does not find resolution directly with their Provider or via CRRS, they may submit a formal complaint to the Department. Participants can submit complaints to the Department by:

- completing an online [complaint form](#)
- sending an email to complaints@dss.gov.au
- sending a letter to DSS Feedback, GPO Box 9820, Canberra ACT 2601
- calling the Feedback Coordination Team (FCT) on 1800 634 035 – when calling outside of business hours (9am-5pm Canberra time), callers have the choice of leaving a voicemail to receive a callback within 2 Business Days
- calling TIS National on 131 450 for languages other than English, or
- speak and listen on 1300 555 727 then ask for 1300 362 072.

When the Department is investigating feedback or a complaint, Providers must:

- actively help in the Department’s investigation of the matter
- engage in negotiating a resolution of the feedback or complaint, including, where needed with other authorities, if the relevant Participant has chosen to utilise other legislative or administrative complaints mechanisms, and



- not withhold Services from a Participant who provides feedback or makes a complaint or discriminate against a Participant because of feedback or a Complaint.

Provider Feedback and Complaints

If the Provider wishes to provide feedback to the Department, the Provider must, in the first instance, provide feedback to their Account Manager. A Provider's Account Manager will consider all feedback and complaints received from their Provider and respond as appropriate.

If the Provider is not satisfied with the Account Manager's response to the Provider's feedback or complaint, the Provider may request the Account Manager to refer the matter to an appropriately senior Department officer. The Account Manager will then refer the matter to an appropriately senior Department officer for consideration and response as appropriate.

If the Provider continues to not be satisfied with the Account Manager's response to the feedback or complaint, the Provider can submit a formal complaint to the Department by:

- completing an online [complaint form](#)
- sending an email to complaints@dss.gov.au
- sending a letter to DSS Feedback, GPO Box 9820, Canberra ACT 2601
- calling the Feedback Coordination Team (FCT) on 1800 634 035 — when calling outside of business hours (9:00 am to 5:00 pm Canberra time), callers have the choice of leaving a voicemail to receive a callback within 2 Business Days
- languages other than English on 131 450 to access TIS National, or
- speak and listen on 1300 555 727 then ask for 1300 362 072.



Chapter 4: Provider Performance Framework

[Supporting Documents](#) for this Chapter

- Inclusive Employment Australia Provider Performance Framework

4.1 Chapter Overview

The Department will assess Provider performance using the Inclusive Employment Australia Provider Performance Framework (Performance Framework).

The Performance Framework assesses provider performance to support participants to find and maintain sustainable employment.

This Chapter outlines the Performance Framework and how the Department will assess Provider performance, including the Key Performance Indicators (KPIs).

Further information about the Performance Framework will be published on the [Department's website](#) once finalised.

4.2 Provider performance

4.2.1 Performance monitoring and assessment

Provider performance is monitored and assessed by the Department on a regular basis and considers a range of factors. The Department assesses Provider performance against each KPI in the Performance Framework — refer to Section 4.2.2 Key Performance Indicators.

To inform the assessment of a Provider's performance, the Department will use data collected through the Department's IT Systems, as well as information and data collected from sources, such as feedback from Participants and Employers. The handling of feedback is managed as outlined in the Deed.

The Department may provide feedback to the Provider on the Department's assessment of its performance, including if the Department considers the Provider's performance is such that it is likely to be in scope for an extension or non-extension of any deed terms.

The Department may periodically initiate broader reviews of the Performance Framework. Such reviews could result in the Department making changes to the Performance Framework, such as adding, removing or adjusting measures.

(Deed Reference(s): Clause 35, 52, 169)

4.2.2 Key Performance Indicators

The Key Performance Indicators for the Performance Framework are under development.

(Deed Reference(s): Clause 169.4)

4.2.3 Scoring performance

Performance reporting has been designed to promote transparency and clarity in the way Provider performance is assessed. This is achieved through the distribution of Provider Performance Scorecards.



Performance Scorecards communicate Provider performance against each KPI. They serve as a critical tool for advancing service quality and enhancing outcomes in the disability employment sector. Providers will receive a rating for each KPI. The table below details definitions for the ratings.

Rating Definitions

Rating	Details
Exceeds	Providers are exceeding the Department's expectations.
Meets	Providers are meeting the Department's expectations.
Improvement Required	Providers have not fully met the Department's expectations. Improvement actions are required or will continue.
Insufficient Data	Providers did not have enough participants to be able to show a score, or the score is not being measured.

Information collected about Provider performance will also be used by Government to monitor overall program performance.

4.2.4 Release of Performance Scorecards

Performance Scorecards are released quarterly on the Department's website.

4.3 Performance Management

The Department is committed to fostering a collaborative environment with Providers and stakeholders to support the measurement, promotion of best practice, and continuous improvement of program performance. Active engagement from Providers is essential as it enables ongoing development and contributes to the achievement of the program's objectives.

To ensure a high standard of service delivery, the Department will regularly assess Provider performance. These evaluations are critical in identifying providers who are either exceeding or not meeting established performance benchmarks.

Providers are encouraged to review their performance regularly to gain a clear understanding of their current standing and identify areas for improvement.

Where performance falls below expectations, the Department may implement targeted actions to address identified issues.

4.3.1 Provider Performance Monitoring

The Department will monitor performance in accordance with evaluation activities and performance assessments of the Deed, including:

- performance reviews against each KPI
- random and targeted assurance activities
- ongoing monitoring of compliance against the Deed, and
- ensuring compliance and quality of service against the NSDS — refer to Part A Guidelines: Chapter 3: Provider Servicing Standards for more information about the NSDS.

(Deed Reference(s): Clause 170 and Clause 171)



4.3.2 Compliance and Performance Improvement

When a Provider first receives any compliance non-conformities or Improvement Required against the KPIs, the Department will work with the provider to identify potential causes and develop strategies for improvement.

4.3.3 Performance Improvement Plans

Where a Provider has three consecutive performance ratings of 'Improvement Required' for a KPI, they must initiate a Performance Improvement Plan (PIP) with the Department. The Department has discretion to ask Providers to amend PIPs as appropriate.

PIPs must describe the actions Providers will implement to improve the performance for which they have a rating of 'Improvement Required'. At a minimum PIPs must outline:

- the Performance Framework measure, outcome(s), and indicator(s) which require improvement
- a description of areas for improvement
- actions to address the areas to improve quality
- who is responsible, and
- timeframes.

4.3.4 Performance Review and Business Reallocation

The Department will undertake formal performance assessments regularly and has the right to take corrective action if it deems the Provider's performance to be less than satisfactory at the service level.

The purpose of the formal performance assessment is to ensure Participants continue to access a highly effective and efficient service for the remainder of the Deed. Delivery of effective program services is a key factor in enabling job seekers with disability to take up appropriate employment opportunities.

The Department will exercise its discretion to discontinue services reasonably and in good faith as set out in the Deed. The Department intends to discontinue services only where it considers, based on available information, that the service cannot reasonably deliver an acceptable service to participants.

The Department has absolute discretion to take these actions, and they do not limit the other rights under the Deed or at law.

(Deed Reference(s): Clause 169.6 and Clause 170)



Chapter 5: Record Management Instructions

[Supporting Documents](#) for this Chapter

- [Employment Services Records Disposal Authority 2003/00330307](#)
- [Employment Services Records Authority 2009/00179260](#)
- [General Records Authority 31 - Destruction of source or original Records after digitisation, conversion or migration](#)
- [General Records Authority 33 – Accredited Training](#)
- [Guide to securing Personal Information](#)
- Privacy Incident Report

5.1 Chapter Overview

This Chapter outlines Provider obligations regarding the creation, management, retention, storage, transfer and disposal of Records created or used by Providers under the relevant Deed, and access to those Records by its Personnel and Subcontractors, in accordance with the Records management provisions in the relevant Deed. Providers must create and maintain true, complete and accurate Records in connection with the delivery of its obligations under, and in accordance with the relevant Deed and these Records Management Instructions.

For the relevant Deed, this Chapter of the Guidelines is the Records Management Instructions.

General advice on the management and storage of Records, information and data is available on the [National Archives of Australia \(NAA\)](#) website.

5.2 Records Framework

Under the relevant Deed, 'Records' means documents, information and data stored by any means and all copies and extracts of the same. Records include 3 categories:

- **Commonwealth Records** are Records provided by the Department to Providers for the purposes of the relevant Deed and includes Records which are copied or derived from Records so provided.
- **Deed Records** are all Records:
 - created for the purpose of performing the relevant Deed
 - incorporated in, supplied or required to be supplied along with the Records referred to in the point above, or
 - copied or derived from Records referred to in the above points, and
 - includes all Reports, as defined in the relevant Deed.
- **Provider Records** are all Records, except Commonwealth Records, in existence prior to the relevant Deed Commencement Date that are:
 - incorporated in
 - supplied with, or as part of, or
 - required to be supplied with, or as part of, the Deed Records.

To the extent that Records contain Personal Information for the purposes of the *Privacy Act 1988* (Cth), Providers must take reasonable steps to ensure that any Personal Information:



- collected is accurate, up-to-date and complete, and
- used or disclosed is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

5.2.1 General Records Authority 40

The General Records Authority 40 (GRA 40) sets out the requirements for the transfer of custody of Commonwealth Records to contractors providing Services under outsourcing arrangements, either on behalf of or to the Australian Government. The GRA 40 provides that, notwithstanding custody of Records that temporarily resides with the Provider, ownership of the relevant Records remains with the Australian Government.

Further information on relevant application and conditions of the GRA 40 is provided on the [NAA website](#).

5.3 Management of Records

In accordance with the "digital by default" approach set out in the Australian Government's *Building trust in the public record: managing information and data for government and community* policy (effective 1 January 2021), Providers must, wherever possible and consistent with the Deed and other applicable legal requirements, create and manage Records in a secure digital format.

Providers must ensure that any digital Record is created, stored and operated in accordance with the Deed requirements (particularly the requirements in relation to Provider IT Systems and other applicable legislative provisions, including the [Electronic Transactions Act 1999 \(Cth\)](#)).

Digital Records containing sensitive information as defined in the [Privacy Act 1988 \(Cth\)](#) must be kept securely. The [Office of Australian Information Commissioner \(OAIC\)](#) website provides information on keeping personal identifying information secure.

The Provider must ensure its:

- Personnel, Subcontractors or Third-Party IT Vendors do not access, copy, disclose or use any:
 - Record containing any information about any employment services program Participant, or
 - Record in the Department's IT Systems containing any information about any individual (including individuals who are not Participants in any employment services program),

unless such access, copying, disclosure or use is for the purpose of:

- providing Services to a Participant under the relevant Deed, or
- otherwise complying with the Deed.

Where a provider offers communal computers for use by participants, the provider must ensure there is a procedure to prevent personal information being retained and accessible on the computer.

If a Provider was a Provider under the DES Grant Agreement 2018-2024 and continues to provide Services to Participants under the relevant Deed, the Provider must comply with the relevant Deed in the use and management of Records.



5.3.1 Storage of Documentary Evidence in the Department's IT Systems

Providers must have true, complete and accurate Documentary Evidence to prove the Provider:

- is entitled to the Payment
- has delivered the Services relevant to the claim for Payment, and
- has done so in accordance with the Deed and these Guidelines.

Key requirements for collecting, retaining and submitting Documentary Evidence include:

- Providers must retain sufficient Documentary Evidence to provide proof of claims of payment
- Providers must ensure they comply with their Privacy obligations
- The Department may contact other relevant people, such as Employers or Participants, to verify the Documentary Evidence provided by the Provider
- Providers must take all necessary steps to verify the truth, completeness and accuracy of Documentary Evidence, and
- Any data entered into the Department's IT Systems must be consistent with the Documentary Evidence held by the Provider.

(Deed reference(s): 24.4, 25, 34)

Documentary Evidence successfully uploaded to the Department's IT Systems is retained by those IT Systems and the Provider does not need to retain a copy.

Where the Deed or these Guidelines specify that Documentary Evidence is required, Providers must either:

- upload Documentary Evidence against the claim, or
- link to previously uploaded Documentary Evidence.

Use of File Notes

Providers must use verifiable Documentary Evidence wherever possible. File Notes may be accepted:

- to provide context for other verifiable evidence, such as explaining the use of a purchased item, or setting out reasons why a Special Claim was required. File Notes may not be used to substitute for verifiable evidence, such as asserting that an item was purchased, or
- in exceptional circumstances, to record required details of a Job Placement. In this case the Provider must also upload additional file evidence (not through another File Note) demonstrating to the Department's satisfaction:
 - verifiable evidence was sought and is not available, and
 - the exceptional circumstances that led to verifiable evidence not being available.

While a Provider must show they attempted to obtain verifiable evidence from the Employer and the Participant, inability to obtain that evidence does not of itself demonstrate to the Department's satisfaction that there are exceptional circumstances justifying a File Note. As the Department's satisfaction with File Notes and associated evidence cannot be checked in advance, Providers accept the risk that claims supported by File Notes may be recovered by the Department.



Where Providers manage File Notes through an approved IT System, the system must ensure File Notes have a date, time and user stamp on the entry, and these details are included in extracts or printouts uploaded to the Department's IT Systems as Documentary Evidence.

Use of Employer or Participant Statements

These Guidelines allow, as Documentary Evidence for Outcome Fees and some related Fees, a "signed and dated written statement or email" from an Employer or Participant containing specified details. In this form of Documentary Evidence, the Employer or Participant is asserting the details in the written statement or email are correct.

A written statement containing required details is acceptable where the Employer or Participant signs and dates the page or pages containing the details.

A statement by email containing required details is acceptable where the email is sent by the Employer or Participant making the statement (including in response to a previous email) and:

- includes within the body of the email both the required details and a statement from the person (Employer or Participant) that the details are correct
- attaches a scanned copy of a written statement containing the required details that has been signed and dated by the person (Employer or Participant), or
- attaches a document containing the required details and includes within the body of the email:
 - matching summary details, including the Employer and Participant names, period covered by the document and total hours and earnings specified in the document, and
 - a statement from the person (Employer or Participant) that the details in the attached document are correct.

Consent to contact an Employer

Most Documentary Evidence must be collected from either the Participant or their Employer (or other relevant organisation). A Participant can choose to not give permission for their Provider to collect Documentary Evidence – for example, if the Participant does not wish to disclose their disability. In this case, the Inclusive Employment Australia Provider must obtain verifiable evidence from the Participant.

To support best practice:

- Where Documentary Evidence is a hard copy (paper statement or form), whiteout must not be used, and any alterations or amendments must be signed and dated by the signatory
- Where Documentary Evidence is an email, the Employer or Participant must be clearly identifiable as the sender in the email address and/or the signature block, and
- Signature blocks must state the person's name and, where applicable, the person's contact phone number, email address, position and organisation. Signature blocks for emails do not need to include an electronic signature.

(Deed reference: 25)



5.3.2 Storage Requirements

The Provider must store all Records in accordance with these Records Management Instructions, the Department's Security Policies, and where relevant, its *Privacy Act 1988* (Cth) and *Archives Act* obligations.

Providers must store Records securely either on their own premises or off-site using a records storage facility in compliance with legislation covering the management of Commonwealth/Deed Records, including the *Privacy Act 1988*.

For Records that contain Personal Information for the purposes of the *Privacy Act 1988*, the Provider must take such steps that are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure. The guide to securing Personal Information can be found on the [OAIC website](#) and provides guidance on the reasonable steps entities are required to take under the *Privacy Act 1988* to protect the Personal Information.

Providers must ensure the Department can access Records by retrieving the Record (including, if stored digitally, by retrieving the digital copy and if relevant printing it) and providing it to the Department upon request.

Providers are required to store digital Records in accordance with the Department's Security Policies, including the Security Policy for External Employment Service Providers and Users available on the Provider Portal.

General advice on the management and storage of Records is available on the [NAA website](#).

Providers must ensure physical Records are protected from:

- unauthorised addition, alteration, removal or destruction
- use outside the terms of the relevant Deed
- for Records containing Personal Information, incidents of privacy, and
- unauthorised access including inappropriate 'browsing' of Records.

Physical Records containing sensitive information, as defined in the *Privacy Act 1988*, must be kept in lockable cabinets.

5.3.3 Control of Records

Providers must be able to locate and retrieve Records about a Participant if requested. Providers must inform their Account Manager if they become party to legal action in relation to their previous or current delivery of Services, so that arrangements for the appropriate retention of Records can be organised.

Providers must store Records in such a way that all Records relevant to a request under the [Freedom of Information Act 1982 \(Cth\)](#) or under APP 12 of the *Privacy Act* are able to be located and retrieved efficiently. This includes being able to retrieve email Records and Records created by, or sent to, individuals who have ceased working for Providers.

Records Register

The Provider must maintain an up-to-date register of the Records (digital and physical) held by the Provider and any Third-Party IT Vendor and make this register available to the Department upon request. The register should contain sufficient information to clearly identify the content and location of a Record.



The Records register must be created and managed in a digital format (ideally Microsoft Excel or equivalent or a comma or tab delimited format) that the Department's IT Systems can read. Providers may wish to identify on the Records register whether Records are:

- Priority — pertaining to current or pending legal action, complaint, injury or possible claim for compensation
- Active — current Participants
- Inactive — former Participants
- Damaged — e.g. paper Record affected by water
- Destroyed (whether authorised or accidental) — e.g. paper Record burnt
- Transferred — Participant and Record transferred to another Provider, and
- Returned — have been returned to the Department.

5.4 Movement of Records

The Provider must not, and must ensure that its Personnel do not:

- take, transfer, transmit or disclose any Records relating to the Services, or
- allow any Records relating to the Services to be taken, transferred, transmitted, accessed or disclosed

outside of Australia without the Department's prior written consent.

Further, the obligation set out above applies in respect of taking, transferring, transmitting, accessing or otherwise disclosing any Records relating to the Services outside of Australia by the Provider:

- within the Provider's Own Organisation, and
- to any third Party, including to any Subcontractor.

5.5 Transfer of Records

Providers must only transfer the Records in accordance with these Records Management Instructions or as otherwise directed by the Department.

5.5.1 Transfer between Providers

Records (digital or physical) must only be transferred between Providers in accordance with the relevant Deed and these Records Management Instructions, and where it is required to continue providing Services to Participants. Records must be transferred securely by Providers, as soon as possible or within 28 days of a request to transfer Records. A list of all Records being transferred should be provided to the receiving Provider.

The transfer of Records containing Personal Information and Protected Information must be in accordance with the *Privacy Act 1988* and the [Social Security \(Administration\) Act 1999 \(Cth\)](#).

When a Provider is transferring Records between its Sites, to another Provider, for storage or secure destruction or to the Department, it remains the Provider's responsibility to ensure the Records are secure during the transfer process.



5.6 Data Migration

Data migration is the process of transferring data from one application or format to another. It may be required when implementing a new application.

Providers must ensure any migration activities include validation of the migrated data quality to ensure that no data is lost and the data continues to be fit for its intended purpose.

When migrating information Providers must ensure:

- the migration is planned, documented and managed
- pre and post migration testing proves that authentic, complete, accessible and useable Records can and have been migrated, and
- source Records are kept for an appropriate length of time after the migration to enable confirmation that the migration has been successful. Determination of the specific retention period must be based on an organisational risk assessment.

Providers must note that the information transferred to the Department will be imported into the Department's official recordkeeping system and appropriate classification will be applied at the time of import.

5.6.1 Data Security Considerations

Providers are responsible for ensuring Records and any data contained in those Records are secure and appropriately accessed. Providers should ensure:

- those who access Sensitive or Protected Information have an appropriate security clearance and a need to know that information
- access (including remote access) to supporting IT systems, networks, infrastructure and applications is controlled
- information in systems is continuously safeguarded from cyber threats, and
- administrative privileges such as logon and administrator privileges are restricted.

Providers should refer to the digital Information Assurance / IT Security Compliance guide on the [Department of Employment and Workplace Relations' website](#) for more information.

(Deed reference(s): 42.17 - 42.23)

5.6.2 Decommissioning of Systems

When decommissioning any internal systems and migrating Records to a new or updated system, Providers should ensure processes are in place to prevent the loss, destruction or corruption of those Records. If Records have been identified for destruction a Provider must obtain the consent of the Department prior to the destruction, unless:

- the Record is not a Record created in accordance with the Deed
- the Record has been successfully uploaded into the Department's IT Systems in accordance with the Deed, or
- otherwise specified by the Department in writing.

If in doubt, the Provider should consult with the Department via the Account Manager.

Digital preservation requires a proactive program to identify Records at risk and take necessary action to ensure their ongoing viability. To achieve this, the Providers must



consider the lifecycle of the information versus the lifecycle of the system and have plans in place to preserve information as needed. Regular and planned migration helps avoid obsolescence and ensures information continues to be accessible and useable.

5.7 Breaches and Inappropriate Handling of Records

5.7.1 Reporting Requirements

Providers must report to the Department all incidents involving Records, including unauthorised access, damage, destruction, loss or theft. Where the Records contain or possibly contain Personal Information of Participants, Providers must follow the Privacy incident reporting process set out in [Chapter 6: Privacy](#).

5.7.2 Rectification Requirements

For all incidents involving the misuse, interference, loss, unauthorised access, unauthorised use, unauthorised disclosure, damage, destruction, loss or stealing of Records (digital or physical), Providers must:

- immediately Notify the Department, giving details of the actual, suspected or possible Breach
- immediately make every effort to recover lost or damaged Records (e.g. retrieving or photocopying Records), including if required, arranging and paying for the services of expert contractors (e.g. disaster recovery or professional drying services)
- not destroy damaged Records without prior authorisation from the Department
- inform Participants if any Personal Information has been lost or is at risk of being publicly available
- where relevant and if necessary, reinterview Participants to recollect information, and
- review relevant policies and procedures to ensure their adequacy in future.

The Department may make recommendations to the Provider to mitigate the risk of recurrence of the incident.

(Deed reference(s): 46)

5.7.3 Notifiable Data Breaches

If a Provider becomes aware there are reasonable grounds to suspect there may have been an eligible data Breach in relation to any Personal Information held by the Provider in its performance of the Services under the Relevant Deed, the Provider must, as soon as possible and in any event within two calendar days, notify the Department as set out in the Deed.

Please refer to the Chapter 6: Privacy [for further information on responding to a Notifiable data Breach](#).

(Deed reference(s): 45.6 - 45.7)

5.8 Retention of Records

All Records must be retained by the Provider for a period of no less than 7 years after the creation of the Record, unless otherwise specified in the Relevant Deed or these



Records Management Instructions or advised by the Department in accordance with the *Archives Act*.

For certain Records, specific retention periods may be applicable in accordance with [Employment Services Records Disposal Authority 2003/00330307](#), [Employment Services Records Authority 2009/00179260 \(RA\)](#) and the [General Records Authority GRA 33 Accredited Training 2012/00579704 \(GRA 33\)](#).

Records with a longer retention period should be maintained by the Provider until they no longer require them and then be returned to the Department for ongoing management. Records in storage arrangements that are retrieved should be converted to digital format and the physical record destroyed.

Providers have the discretion to retain Records longer than the minimum periods required by law but must not destroy Records prior to the expiration of the relevant retention periods. In addition, the Department may direct some Records to be retained for longer periods, for example, in the case of Records required in any legal action.

Providers must review Records that have reached the minimum retention period before destroying them in accordance with these Records Management Instructions.

If a relevant Record has reached the required minimum retention period but, for example, the Provider has knowledge of a legal action or potential legal action, the Provider must re-sentence the Record and inform the Account Manager. Sentencing is the process for identifying the minimum retention period for a Record by assessing them against the classes specified in the relevant Records Authority.

At the Completion Date, the Provider must manage all Records in accordance with these Records Management Instructions, the Relevant Deed or as otherwise directed by the Department.

Retention periods are determined with reference to NAA accredited records authorities.

5.9 Destruction of Records

The Provider must:

- not destroy or otherwise dispose of Records, except in accordance with the Deed, these Records Management Instructions or as otherwise directed by the Department, and
- provide a list to the Department of any Records that have been destroyed, as directed by the Department.

Records must not be destroyed where the Provider is aware of current or potential legal action or where the Records are subject to a [Disposal Freeze or Retention Notice](#) issued by the NAA, even if the minimum retention period has been reached. These Records are priority Records and must be retained in accordance with requirements set out for priority Records in [Control of Records](#) section. A Provider must also comply with any Direction from the Department not to destroy Records. Providers must only destroy Records that have reached the minimum retention period and following the review process outlined in [Retention of Records](#) section.

Providers must maintain a list of destroyed Records which must be supplied to the Department upon request. This list must also be retained by the Provider in accordance with the applicable retention period or as directed by the Department.

Refer to [Retention of Records](#) section for information on retention periods.



5.9.1 Methods of destroying Records

When Providers destroy Records, they must use a method that ensures the information is no longer readable and cannot be retrieved.

Digital Records

It is the Provider's responsibility to ensure all digital Records are identified and removed from their systems and destroyed. Methods of destroying digital Records include:

- file shredding
- degaussing — the process of demagnetising magnetic media to erase recorded data
- physical Destruction of storage media — such as pulverisation, incineration or shredding, and
- reformatting — if it can be guaranteed the process cannot be reversed.

To ensure the complete Destruction of a digital Record, all copies should be found and destroyed. This includes removing and destroying copies contained in system backups and off-site storage.

Deletion is not destruction and does not meet the requirements for Destruction of Australian Government Records. When digital Records are deleted, it is only the pointer to the Record (such as the file name and directory path) that is deleted. The actual data objects are gradually overwritten in time by new data. However, until the data is completely overwritten, there remains a possibility that the information can be retrieved.

Physical Records

Providers must ensure physical Records are destroyed using one of the following methods:

- pulping – transforming used paper into a moist, slightly cohering mass
- burning – in accordance with relevant environmental protection restrictions, and
- shredding – using crosscut shredders (using either A or B class shredders).

If Destruction of physical Records is undertaken at an off-site facility, then a certificate of destruction including details of the Records destroyed and appropriate authorisation must be obtained and retained by the Provider.

5.9.2 General Records Authority 30

Records may be damaged beyond repair because of a disaster, emergency, or other unforeseen circumstance, as defined in GRA 30.

If a Provider considers that a Record or Records have been damaged in line with GRA 30, it must not destroy the Record(s) unless and until the Department provides written authority for the destruction of the Record(s). Providers must notify the Department as soon as possible following the Record(s) being damaged, providing at a minimum:

- photographic evidence of the damaged Record(s)
- do any of the damaged Record(s) need to be retained permanently
- information about the circumstances causing the damage, including whether:
 - the Record(s) in their damaged state pose a health hazard, and
 - any Record(s) were able to be retrieved following the circumstances causing the damage and if so, how this retrieval will be managed.



- information about the Record(s), including:
 - the number affected, and if approximated, how this number was determined
 - their content
 - their classification, and
 - whether they had been digitised
- information about how the damaged Record(s) are proposed to be destroyed, and
- any other information the Provider considers relevant to a request to destroy the Record(s).

5.9.3 General Records Authority 31

Records as defined in the Deed are Commonwealth Records for the purposes of the *Archives Act 1988* (Cth).

Subject to certain exclusions and conditions, the NAA provides permission for the destruction of Commonwealth Records created on or after 1 January 1980 under General Records Authority 31 -Destruction of source or original Records after digitisation, conversion or migration (GRA 31) where those Records have been converted from hard copy to digital form.

Providers, as 'authorised agents' of the Department, must comply with the requirements of GRA 31.

Providers must retain the original copy of a paper Record for the relevant retention period and return it to the Department in accordance with this Chapter, regardless of whether it has also been converted to digital form, if required to do so under relevant Deed/s, Guidelines or if directed by the Department. Further explanation of the relevant conditions and exclusions for [GRA 31](#) is available on NAA website.



Chapter 6: Privacy

[Supporting Documents](#) for this Chapter

- Privacy Notification and Consent Form
- Direct Registration Form
- Release of Protected Information Notification Form
- Provider Privacy Incident Report
- Public Interest Certificate (PIC)
- [Public Interest Certificate \(PIC\) Guidelines](#)

6.1 Chapter Overview

This Chapter provides information for Providers, their Personnel and Third Parties on their obligations in relation to handling Personal and Protected Information about individuals, as well in relation to reporting privacy incidents.

6.2 Where to find your obligations

When a Provider enters into a Deed with the Commonwealth to deliver Services, the Provider becomes:

- a “service organisation” with obligations about Protected Information under the *Social Security (Administration) Act 1999* (Cth) (the **Social Security Law**), and
- a “contract service provider” with obligations about personal information under the *Privacy Act 1988* and the Australian Privacy Principles (the **privacy law**).

A Provider may also have other obligations about how to handle information under the laws of States or Territories where it operates as well. It is the Provider’s obligation under the Deed to make sure that it understands and complies with all its legal obligations when delivering the Services.

Privacy obligations

The privacy law sets minimum standards for handling personal information, known as the Australian Privacy Principles (APPs). The Office of the Australian Information Commissioner (OAIC) has published guidelines about the APPs and what they mean — see the [OAIC website](#).

As the Provider is delivering work-related services to participants under the Deed with the Commonwealth, the Provider is a contract service provider and must meet the same APP requirements as a Commonwealth agency (rather than the APP requirements of an organisation).

If the Provider subcontracts any delivery of services to another organisation, then the Provider must make sure the subcontractor also meets the same APP requirements as a Commonwealth agency.

In delivering Services, Providers collect, use and disclose personal information about individuals. The APPs includes standards, rights and obligations around the:

- management of Personal Information
- collection, use and disclosure of Personal Information
- the security of Personal Information, and
the rights of individuals to access and correct their Personal Information.



The APPs are principles-based law. The Provider must consider its own situation and relevant Deed provisions and implement procedures and policies to ensure compliance with the relevant APPs, noting that their obligations may be different as a contract service provider to those as an organisation undertaking other business activities.

The Provider and its Personnel must also make sure they comply with their obligations in relation to the tort of serious invasion of privacy, in Schedule 2 of the Privacy Law.

(Deed Reference(s): Clause 45)

6.2.1 Personal information and sensitive information

The *Privacy Act 1988* defines “personal information” as:

information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, or is recorded in a material form or not. [What is personal information? | OAIC.](#)

Personal Information includes an individual’s name, signature, date of birth, address, telephone number, sensitive information, bank account details, employment information, and commentary or opinion about an individual. This kind of information may be shared verbally, contained in physical or digital files or documents, such as résumés or application forms provided by the individual, or in an email or text message, or recorded.

Sensitive Information is a subset of personal information and includes information that relates to an individual’s racial or ethnic origin, health status, genetics and biometrics, religious beliefs or affiliations, philosophical beliefs, sexual orientation, criminal record or membership of a political association, professional or trade association or trade union.

Sensitive Information is subject to higher levels of protection under Privacy Law.

Information about a person’s disability is generally considered to be Sensitive Information’, because it is a kind of information about a person’s health – see [What is health information?](#) This means Providers will be handling ‘sensitive information’ as part of delivering the Services and need to ensure their practices, procedures and systems meet the higher privacy standard required. Providers should make sure they are also meeting any obligations about the handling of ‘health information’ under State or Territory law.

6.2.2 Consent and the APPs

In complying with the *Privacy Act 1988*, the APPs and this Chapter, it will be important for Providers to get consent from individuals for the handling of their personal and sensitive information.

In all cases, the Provider must ensure when it asks a person for their consent for the handling of their personal and sensitive information:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

Consent can be given expressly, either orally or in writing, or it can be implied. In whatever way the person gives their consent to the Provider, the Provider must record



the consent so that it can be found and checked easily in the day-to-day operations of the provider and if the Department requires to see it. As described at 5.3.1 Storage of Documentary Evidence in the Department's IT Systems, the best way to do this is to record the consent and how it was obtained in the Department's IT system, where possible.

Please see 6.3.1 Participant consent requirements for requirements about the method of obtaining and recording participant consent prior to their commencement in the program.

Providers must establish a person's capacity to give consent on a case-by-case, decision-by-decision basis. A person's capacity to give consent can be affected by their age or the nature of their disability (e.g. people with an intellectual disability may be unable to give consent). Further, a person's ability to give consent may change over time. A Provider must prepare practical guidance for their Personnel, which includes options for supported decision making, so Participants can make their own decisions about their personal information. As a guide, the Department recommends Providers familiarise themselves with the NDIA Supported Decision Material, available here: [National SDM Guide](#).

Where an individual is under 18 years old, the Provider must decide if the individual has the capacity to consent on a case-by-case basis. The [OAIC](#) advises, as a general rule, that an individual under the age of 18 has the capacity to consent if they have the maturity to understand what is being proposed. If the individual lacks maturity, it may be appropriate for a parent or guardian to consent on their behalf.

A Provider's ability to rely on a person's consent diminishes over time. Providers must ensure each individual's consent is regularly reviewed on an ongoing basis (such as in relation to the collection and disclosure of sensitive information under the Privacy Statement contained in the [Privacy Notification and Consent Form](#) and/or [Direct Registration Form](#), see [APP 3: Collection of solicited personal information](#) below). This process should typically occur annually.

Further information about consent can be found on the [OAIC's website](#).

6.3 APP 3 and 5: Collection of solicited personal information

APP 3 outlines when an APP entity may collect solicited personal information, including sensitive information.

To deliver the Services they are contracted to provide, Providers are generally required to collect personal information. APP 3 outlines when an APP entity may collect solicited personal information, including sensitive information (see 6.2.2 Consent and the APPs).

Providers may only solicit and collect personal information that is reasonably necessary for, or directly related to, one or more of the Provider's functions or activities. A Provider's functions or activities will vary depending on the Services being delivered and Providers should consider their obligations under their Deed(s) with the Department to deliver Services before collecting personal information.

APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps to notify the individual of certain matters or to ensure the individual is aware of those matters.



As well as obtaining their consent to the collection of sensitive information as required by APP 3, the Privacy Notification and Consent Form and Direct Registration Form (discussed below at 6.3.2 Consent to the collection of Sensitive Information) complies with APP 5.2 by informing the individual of matters such as:

- the identity and contact details of the Department
- the purposes for which the Department and Provider are collecting the personal information, and
- the main consequences for the individual if all or some of the personal information is not collected by the Department and Provider.

The provider must not alter the Privacy Notification and Consent Form and Direct Registration Form. If the Department gives the Provider a template for an APP 5 notice and/or consent form, then the Provider must adopt or adapt that form in a manner that meets its obligations under the privacy law. In any event, all privacy and consent documents presented to Participants must use simple language and formatting as much as possible.

6.3.1 Participant consent requirements

In all instances, before providing employment services to Participants (new or transferred), Providers must provide Participants with the standard Privacy Notification and Consent Form or Direct Registration Form as appropriate. Providers must ensure they are using the most up-to-date form.

Providers must obtain the Participant's consent and declaration in accordance with the Privacy Notification and Consent Form or the Direct Registration Form, as appropriate, before handling the Participant's personal and sensitive information, commencing a Direct Registration process and/or providing them with employment services. In addition, the Provider must ensure that the Participant's consent is current and checked for currency every 12 months or in changes of circumstances.

During the first meeting or interview with the new or transferred Participant, the Provider must:

- issue the Participant with the appropriate standard Direct Registration Form or Privacy Notification and Consent Form
- discuss and explain the contents of the form, answering any questions the Participant may have, in a manner that meets the Participant's communication needs
- ensure that the Participant understands in accordance with the Privacy Statement:
 - the types of personal information collected, and how it will be used and disclosed as part of the program
 - the Provider collects this information to commence the participant in the program or otherwise determine if the person is eligible to receive the Services, and will use the information to check whether the person already has a record in the Department's IT Systems
 - they are not required to give consent for the collection of their Sensitive Information and can withdraw their consent at any time
 - that Services provided may change depending on whether personal information is given or consent is withdrawn



- that withdrawing their consent may ultimately affect their participation in the program, and affect any mutual obligation requirements
- which third parties have access to information in the Department's IT Systems, and
- if eligible, the Provider will use the information to register the person to start receiving the Services.
- ensure they are satisfied that the Participant (or their Legal Guardian or authorised nominee) has provided valid consent to how their personal information will be handled in accordance with the Privacy Statement in the relevant form
- ensure the Participant agrees to the Participant declaration in the appropriate form
- ensure they otherwise comply with and agree to the Provider declaration in the appropriate form at the same time as the Participant, and
- otherwise ensure the Participant provides valid consent consistent with the requirements of the *Privacy Act*.

Participant does not provide consent

If a Participant does not wish to provide consent at the first meeting (for example they want to seek further information about how their information will be used so they can provide informed consent) they can provide a record of their consent at a later date but should be made aware that this will delay their ability to commence in the program. Implied consent is not sufficient to commence the participant or begin providing them with employment services.

Recording the Participant's consent

Providers must ensure that a record is made of the Participant's valid and express consent to have their information handled in accordance with the Privacy Statement in the Direct Registration Form or Privacy Notification and Consent Form. This record of consent should then be scanned and/or uploaded to the IT system. The preference is for Participants to record their consent via a hard copy or digital form. However, the Participant's consent can be recorded in an alternative format to meet accessibility requirements.

Provided the Participant is providing express consent on the basis of information contained in the Direct Registration Form or Privacy Notification and Consent Form, has agreed to the contents of the declaration, and the Provider has complied and agreed to the declaration at the same time, a Participant's consent can be recorded by:

- completing and signing a hard copy form
- completing and signing a digital copy form
- a detailed file note by the Provider that the Participant has provided express verbal consent to the privacy statement
- a written statement or email from the Participant or their nominee outlining they consent to the handling of their information in accordance with the relevant form and agree to the declaration



- I [participant full name] declare I have read and understood the [Direct Registration Form/ Privacy Notification and Consent Form]. I consent to the collection and use of my personal and sensitive information in accordance with the Privacy Statement and Declaration contained in the Direct Registration Form/ Privacy Notification and Consent Form. [DD/MM/YYYY]
- another format as agreed to by the Department to best meet any accessibility requirements.

Where a file note, written statement or email is used to record the Participant's consent, the record should at a minimum include the date and time of consent and be accompanied with a copy of the form provided to the participant, and the Provider's signed declaration.

See also [Inclusive Employment Australia Guidelines: Part B: Chapter 3: Commencements, Transfers, Suspensions and Exits](#).

6.3.2 Consent to the collection of Sensitive Information

Providers must only collect sensitive information where the individual gives consent to the collection, unless another exception applies.

In all other instances after a participant has been commenced and has not otherwise consented to a particular handling of their information, Providers must provide Participants with an APP 5 compliant Privacy Collection Notice. They must obtain the consent of the Participant before handling their sensitive information. In addition, the Provider must ensure that the Participant's consent is current and checked for currency every 12 months or in changes of circumstances. Providers should make it clear to Participants that if they withhold or withdraw their consent, this may ultimately affect their participation in the program or affect any mutual obligation requirements they may have.

Whenever obtaining consent from a Participant, the Provider needs to ensure a Participant is given the time and information they need to understand what is being asked of them, so that the Participant has a real choice. This means the Provider must ensure their Personnel understand privacy and consent documents, so they can explain these in a manner that meets the Participant's communication needs.

The Provider must provide guidance to their Personnel about how to properly identify and manage capacity or other issues which affect a Participant's ability to understand a privacy or consent documents, including how and when to call on a Participant's nominee or use an interpreter.

When signing the Privacy Notification and Consent Form or Direct Registration Form, the Participant indicates consent at the time of signing. Individuals may also provide their express consent to the form verbally. Refer to Section 6.3.1 Participant consent requirements for more information.

In some circumstances, Providers may also reasonably infer from an individual's conduct there has been implied consent to the collection of sensitive information, for example, from the voluntary disclosure of a document containing sensitive information to the Provider. The participant's consent must be recorded in the Department's IT system as an appropriate comment.



Where consent is not provided or is withdrawn and no APP exception applies, the Provider cannot collect the individual's personal information. In these circumstances, Providers must explain to the individual that they may still be required to participate in the program, however the lack of consent may limit the options and employment services that a Provider can offer. For example, if an individual does not consent to the collection of sensitive information about their health status or racial or ethnic origin, they may not be referred to appropriately targeted Specific Cohort services. The Provider must ensure there is a process in place for a Participant to withdraw their consent, which includes providing information to the Participant about what that means for the Participant. This includes the Participant's ability to continue to receive services and any impact relating to mutual obligation requirements or compulsory participation requirements. If they are a voluntary participant and decide to withdraw or withhold their consent, they can exit if they choose.

Some examples of exceptions which may permit the collection of sensitive information without consent include where:

- the collection of personal information is required or authorised by or under an Australian law or a court/tribunal order (e.g. the Social Security Law)
- it is unreasonable or impracticable to obtain the individual's consent to the collection, and the Provider reasonably believes that the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety, or
- the Provider has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the Provider's functions or activities has been, is being or may be engaged in and the Provider reasonably believes the collection is necessary in order for the Provider to take appropriate action in relation to the matter.

The above are examples only. Providers should seek their own independent legal advice before collecting sensitive information without consent or if the Provider is unsure whether the information is a Commonwealth record and should consider the circumstances and obligations under Use and Disclosure of Protected Information below.

Third party consent requirements

Providers must ensure that they do not collect, use or disclose sensitive information about a third party unless:

- the collection is by lawful and fair means
- it is unreasonable or impracticable to collect the personal information directly from the third-party individual
- the third party's personal information is reasonably necessary and required for the Provider to meet its obligations under the deed and these guidelines
- the third party has provided valid consent
- the third party is the Participant's child and is under 15 years of age
- the Participant is the legal guardian of the third party who is under 15 years of age
- the Participant is the legal guardian and authorised decision maker of the third party who may not have capacity to consent, or
- the provider reasonably believes that collection of that sensitive information is necessary to lessen or prevent a serious threat to the life, health or safety of the Participant or any other individual, or to public health or safety, and that obtaining



consent from the third party to the handling of their personal information is unreasonable or impracticable in the circumstance.

Providers may be able to rely on implied consent by third parties in some circumstances where personal information (excluding sensitive information) is provided, e.g. the contact details of an Auslan interpreter.

Providers must make a record of consent by third parties. For example, Providers can upload an email or make a file note that they are satisfied the third party has provided their express consent (e.g. via a phone call) or that their consent is implied.

Before collecting or uploading materials to the IT system containing the personal or sensitive information of a third party, the Provider must be satisfied that appropriate consents have been obtained and make a record of that consent.

Providers must also ensure they redact any sensitive information about third parties which is not reasonably necessary or required, such as Tax File Numbers or Government Identifiers.

6.3.3 Manner of collection

Providers must only collect personal information directly from the individual, unless any one of the following exceptions applies:

- the individual consents to the collection of the information from a third party
- the Provider is required or authorised by Australian law, or court/tribunal order, to collect the information from the third party, or
- it is unreasonable or impracticable to collect the personal information directly from the individual.

For example, it may be unreasonable or impracticable to collect personal information directly from an individual where language difficulties prevent the individual from providing their personal information. In these cases, the Provider should seek the individual's consent to collect the information through an interpreter. Providers must also ensure the use and need for an Interpreter is recorded in the Department's IT system. Under APP 10, Providers are required to take reasonable steps to ensure the personal information they collect is accurate, up-to-date, and complete. Providers therefore need to take steps to ensure the interpreter will be providing accurate and complete information from the individual.

The collection of personal information by a Provider must be by lawful and fair means only. A fair means of collecting information is one that does not involve intimidation or deception and is not unreasonably intrusive.

6.4 APP 4: Dealing with unsolicited personal information

APP 4 outlines when an APP entity may collect unsolicited personal information.

A Provider may receive personal information it did not ask for. APP 4 outlines when a Provider may collect unsolicited personal information. Where a Provider receives unsolicited personal information, it must determine whether it would have been permitted to collect the personal information under APP 3. If not, the Provider must destroy or de-identify the information, unless it is a Commonwealth record under the



Archives Act 1988 or as per the Deed. Most records held by Providers in performing the Services will be Commonwealth records. Providers should seek their own independent legal advice prior to destroying unsolicited information.

If the Provider determines it can collect the personal information under APP 3 or retain the personal information because it is contained in a Commonwealth record, it must handle the information in accordance with the *Privacy Act 1988*.

6.5 APP 6: Use and Disclosure of personal information

APP 6 provides that if an APP entity holds personal information about an individual that was collected for a particular purpose (primary purpose), the entity must not use or disclose the information for another purpose (secondary purpose), unless an exception applies.

Personal information in employment services is generally collected, used and disclosed for the primary purpose, which is administering the relevant employment service program and to provide individuals with appropriate services and assistance. In this case, participant's personal information (including sensitive information) is collected and managed for the primary purpose of administering, managing and regulating the Inclusive Employment Australia program. This includes under any future variation of the Inclusive Employment Australia program (e.g. if the name of the program is changed or if amendments are made to the legislative framework under which the program operates).

A Provider may use and disclose an individual's personal information, including sensitive information, for the primary purpose. More information about the primary purpose can be found in the Privacy Statement in the [Privacy Notification and Consent Form](#) and Direct Registration Form, and information available on the Department's website at [DSS – Participant Privacy](#).

A secondary purpose is any purpose that is not the primary purpose. Providers must not use or disclose personal information for a secondary purpose unless an exception applies, including where:

- the individual consents to the use or disclosure for the secondary purpose*
- the individual would reasonably expect the use or disclosure for the secondary purpose, and either the secondary purpose is related to the primary purpose or, in the case of sensitive information, is directly related to the primary purpose, or
- the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (e.g. the Social Security Law, see 6.9 Use and disclosure of Protected Information).

*It should not be assumed that an individual has given consent on the basis alone that they did not object to a proposal to handle personal information in a particular way.

Access by Provider Personnel to Participant records in the Department's ICT system is a use of personal information and is provided by the Department for the purpose of providing the Services to the Participant only. All access to Department's ICT System by all Provider Personnel can and will be monitored for inappropriate use by the Department, and the Provider must put in place its own systems and processes to protect against this.



The APP 6 obligations apply to the use of personal information by the Provider and the disclosure of personal information to third parties, that is parties other than the Provider. The Provider may disclose personal information, other than sensitive information, to a related body corporate.

6.5.1 Information for 'checks'

Both Provider Personnel and Participants may be involved in activities that have risks which are appropriately managed through background or other checks. These might be checks like police checks, Working with Children Checks, Working with Vulnerable People Checks, Visa Entitlement Verification Online (VEVO) checks, and health/medical checks.

The Provider should make sure that both Participants and their Personnel are notified up-front if a role is likely to involve checks, what those checks are and who the result of a check will be given to. This gives Personnel and Participants more control over whether and what personal information they share, by helping them to identify whether a role is appropriate for them early on.

For both Personnel and Participants, it is the responsibility of the Provider to arrange and pay for all relevant checks, before:

- the person is involved in the relevant activity (in the case of Personnel), and
- the person is involved in the relevant activity or placed in the employment (in the case of a Participant).

When referring an individual to a relevant agency for a check to be undertaken, Providers must ensure the individual is aware their personal information will be disclosed to the relevant agency for this purpose and provide relevant information, including details of what the check will involve. Where a Provider is referring an individual to an activity that requires one or more of these checks, the Provider must refer the individual to the relevant agencies which undertake the checks prior to the placement.

6.5.2 Information for assessments

Participant sensitive information may be collected, used, and disclosed to Health care professionals including the National Panel of Assessors, JobAccess Professional Advisors, Services Australia Assessment Services, or other qualified health and allied health professionals to undertake assessments or provide services as part of the Program. The National Panel of Assessors may undertake:

- Ongoing Support Assessments
- Supported Wage Subsidy Assessments, and/or
- Workplace Modification Scheme Assessments as part of the Employment Assistance Fund.

Providers must ensure that participants are aware that their personal information may be handled by third parties. Providers must also ensure Provider Personnel are aware of and consent to the handling of their personal information by any third parties as required.

6.5.3 Tax File Numbers

Providers and their staff have no requirement to collect a participant's Tax File Number (TFN). If a Participant or Employer supplies a payslip for evidence of outcome fees, payments under a Wage Subsidy Agreement, or to meet any other evidence



requirements, the Provider must not share the TFN with any other party, including the Department.

A Provider must not record, collect, use or disclose TFN information unless this is permitted under taxation, personal assistance or superannuation law. Providers must make themselves aware of when they are authorised to handle TFNs under the TFN Rule and provide appropriate guidance to their Personnel. That guidance must include proper storage and destruction of TFNs, consistent with the TFN Rule.

TFN recipients must take reasonable steps to protect TFN information from misuse and loss, and from unauthorised access, use, modification or disclosure. A breach of the TFN Rule is an interference with privacy under the *Privacy Act 1988*.

Unauthorised disclosure of a TFN may also amount to a breach of [APP 9](#).

6.6 APP 7: Direct marketing

Under APP 7, Providers must not use or disclose personal information for the purposes of direct marketing unless an expressed consent to a secondary collection purpose has been provided by the Participant and recorded. Without express consent, this will consist of a breach, and the Department may take actions under clause 66 of the Deed. It may in some circumstances also constitute an offence in relation to protected information.

Prior to undertaking any direct marketing in relation to functions and activities under the Deed(s), Providers must consider whether the proposed marketing is consistent with the *Privacy Act 1988*. Providers should obtain their own independent legal advice.

6.7 APP 9: Adoption, use or disclosure of government related identifiers

Providers routinely interact with government related identifiers, including Centrelink Reference Numbers (CRNs) and Job Seeker Identification numbers (JSIDs). APP 9 restricts the adoption, use, and disclosure of government related identifiers by organisations. Under the Deed, Providers must comply with APP 9.

APP 9 provides limited exceptions where a Provider may use or disclose a government related identifier of an individual. This means a Provider should make sure it understands its authority in relation to the identifier and provides guidance to its Personnel about how the identifier should be handled. An example is where the use or disclosure of a government related identifier is reasonably necessary for the Provider to fulfil its obligations to the Department.

Providers should note that consent is not a basis on which the adoption, use, or disclosure of a government related identifier may be permitted. Providers should obtain their own independent legal advice.

6.8 APPs 12 and 13: Access to and correction of personal information

Under APP 12, if an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information. APP 12 does not stipulate any formal requirements for making a request or require a request to access personal information be made in writing or require an individual to state it is an



APP 12 request. Therefore, a verbal request for personal information may be a valid request under APP 12.

Under APP 13, if an APP entity holds personal information about an individual and the individual requests the entity to correct the information, the entity must take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Generally, Providers must process requests for access to personal information and requests for correction of personal information. If a Provider receives such a request, they must provide a response within 30 calendar days after the request is made.

Certain requests must be referred to the Department for consideration where the Provider proposes to refuse the request or the request encompass records containing information falling within the following categories:

- records also containing information about another person
- medical records (other than those supplied by the individual, or where the individual has a copy or has previously sighted a copy of the records)
- psychological records, and
- information provided by other third parties (excluding Subcontractors, the Department and Services Australia).

Providers **must not** direct a request to the Department without first considering whether they are obliged to process the request.

If an individual is seeking access to personal information on behalf of another individual, Providers must obtain written authority from the individual whose personal information is being sought before releasing any documents. At a minimum, an authority should state the individual's name, include a description of the documents they are authorising the release of, who the documents can be released to, and bear the individual's signature.

If the Provider is unable to obtain written authority, they should inform the individual they may wish to make a request under the *Freedom of Information Act 1982 (Cth)*.

Requests under the *Freedom of Information Act 1982* should be directed to the Department via FOI@dss.gov.au.

(Deed Reference(s): Clause 50)

6.8.1 Freedom of Information requests

Under the Deed, Providers are required to assist the Department in processing requests under the *Freedom of Information Act 1982* by providing Records (digital or physical) in their possession that are relevant to a request. An individual seeking to access documents containing their personal information may submit a request for access under either the *Privacy Act 1988* or the *Freedom of Information Act 1982*. However, where the document being sought does not contain their personal information, access is not available under the *Privacy Act 1988*. The *Privacy Act 1988* only applies to personal information.

Requests under the *Freedom of Information Act 1982* should be directed to the Department via FOI@dss.gov.au.

(Deed Reference(s): Clause 51.3)



6.9 Use and disclosure of Protected Information

“Protected Information” is defined under the *Disability Services and Inclusion Act 2023* as either:

- (a) personal information within the meaning of the Privacy Act 1988*, or
- (b) information about the affairs of a person the disclosure of which could reasonably be expected to find an action by a person (other than the Commonwealth) for breach of a duty.

* See 6.2.1 Personal information and sensitive information (above).

Both protected information and personal information may be collected, used, and disclosed with the consent of the individual concerned. Compliance with the consent framework for Inclusive Employment Australia is a key part of a Provider ensuring they have authority to deal with information about Participants.

Under Social Security Law, a Provider’s Personnel may obtain, record, use and disclose protected information as part of the efficient and effective delivery of work-related services to Service Recipients. Work-related services include:

- assessment of a Service Recipient’s capacity to work
- helping a Service Recipient prepare to seek or undertake work, and
- placement of a Service Recipient in a position of employment.

Information provided by the Commonwealth through Workforce Australia Online for Providers about a Participant who has mutual obligations will be protected information, that can be handled for the purpose of delivering work-related services being provided under the Deed with the Commonwealth.

6.9.1 Offences related to Protected Information

It is an offence under Social Security Law for a person to intentionally obtain, make a record of, disclose to any other person, or otherwise use, protected information if the person:

- is not authorised by or under the Social Security Law to do so, and
- the person knows, or ought reasonably to know, that the information is Protected Information.

This means the Provider’s Personnel may commit a criminal offence if they:

- search for, or access, Protected Information not required for their duties
- make copies of Protected Information where not authorised
- disclose Protected Information to other staff or third parties who do not need to know that information, or
- otherwise use Protected Information where not permitted.

6.9.2 Permitted uses of Protected Information

Providers are permitted to obtain, make records of, use and disclose Protected Information where this is authorised or required by the Social Security Law, such as:

- for the purposes of the Social Security Law, such as ensuring that an individual enters into, and complies with their Job Plan, or
- to deliver the Services.



Providers may also make a record, use, and disclose an individual's Protected Information where that individual provides express or implied consent to that use or disclosure. This may be helpful where a Provider wishes to assist or support an individual by providing their information with their consent to a third party.

6.9.3 Public Interest Certificates

In addition to the permitted uses discussed above, Providers may disclose Protected Information to certain persons where this is authorised by a Public Interest Certificate (PIC). A PIC identifies the Protected Information that can be disclosed, the purposes for which the information can be disclosed, and to whom the information can be disclosed. A PIC may also specify who can disclose the information.

Protected Information collected prior to 30 June 2025 remains subject to the *Disability Services Act 1986* (Cth). A class PIC, which was issued under the *Social Security (Administration) Act 1999* and paragraph 28(5)(a) of the *Disability Services Act 1986* (Cth), enables disclosure of this information in specified circumstances. For other circumstances, a specific PIC will need to be requested from the Department.

Protected Information collected from 1 July 2025 is subject to the *Disability Services and Inclusion Act 2023*. The Department will issue further instructions in due course regarding the handling of information collected from 1 July 2025.

For detailed information regarding PICs, refer to the [PIC Guidelines](#).

6.10 Privacy Incidents and the Notifiable Data Breaches Scheme

Acts or practices by a Provider which breach an APP are an interference with the privacy of the individual. The OAIC has powers to investigate possible interferences with privacy, either following a complaint by an individual or on the OAIC's own initiative. The OAIC also has a range of enforcement powers and other remedies.

Providers are required under the [Notifiable Data Breaches scheme](#) to notify affected individuals and the OAIC about eligible data breaches. An eligible data breach occurs when there is unauthorised access to, or disclosure of, personal information held by an entity, or information is lost in circumstances where unauthorised access or disclosure is likely to occur.

The Provider must Notify the Department as soon as possible following becoming aware of any unauthorised access to, use or disclosure of, personal information, or a loss of personal information the Provider holds using the [Provider Privacy Incident Report](#) (PPIR). This applies to all privacy incidents, whether or not they are an eligible data breach.

Providers must promptly assess all potential privacy incidents to determine whether an eligible data breach has occurred and, if required, notification is to be provided to affected individuals and to the OAIC. Providers must take all reasonable steps to ensure this assessment is completed within 30 calendar days of becoming reasonably aware of an eligible data breach.

By responding quickly, a Provider can substantially decrease the impact on affected individuals and reduce the costs associated with dealing with the privacy incident, including reputational costs.



The Provider must also provide the Department with a copy of any notification of an eligible data breach made to OAIC and any subsequent correspondence with OAIC.

Providers should refer to the OAIC website for information on the Notifiable Data Breach scheme.

The Provider must also immediately Notify the Department if it becomes aware:

- of a breach or possible breach of any of the obligations contained in, or referred to in the Deed(s) by any Personnel or Subcontractor
- that a disclosure of personal information may be required by law, or
- of an approach to the Provider by the Information Commissioner or by an individual claiming their privacy has been interfered with.

Providers should be aware the Department monitors Personnel access to Records in the Department's IT Systems. Where a clear business reason for access to a Record or Records is not identified, the Department may require further information or investigation by a Provider and may take action against individuals.

6.11 Privacy Complaints

An individual who considers their privacy has been interfered with can contact the Department and/or the OAIC to make a complaint. Where possible, complaints under the *Privacy Act 1988* should be directed to an individual's Provider in the first instance.

Providers are required to respond to any privacy complaints within 10 Business Days and in accordance with the PPIR where a privacy incident has been identified. Providers should follow [OAIC's advice on handling privacy complaints](#).

6.12 Referring individuals to the Department in relation to privacy matters

After first directing their query to their Provider, an individual can contact the Department to query how their personal information is handled, request access to or correction of their personal information, or make a privacy complaint in relation to the Department or a Provider.

Participants can submit a Privacy complaint to the Department by:

- completing an online [complaint form](#)
- sending an email to complaints@dss.gov.au, or
- sending a letter to DSS Feedback, GPO Box 9820, Canberra ACT 2601.

For further details on the complaint process, please refer to 3.6 Complaint processes in Chapter 3 of these Guidelines.

6.13 Awareness and Training Expectations

Providers must adopt practices to ensure its Personnel are aware of their obligations under the privacy law, the Deed and this Chapter. Providers who have access to the Department's IT Systems must ensure that Personnel who handle or will handle personal information in the course of delivering services under the Deed complete the Department's Information Exchange and Privacy Training Module, available on the Learning Centre:



- prior to accessing the IT system,
- prior to delivering the Services, and
- at least once every 12 months.

Providers must also make sure that they provide appropriate notice to their Personnel about how their information will be shared with the Department and other agencies as part of delivering Services to Participants, both as part of the Provider fulfilling its obligations under the Deed and as part of Personnel accessing the Department's ICT system.

Providers should note that the Department's privacy training module has been developed to cater for the delivery of Inclusive Employment Australia. It is not a substitute for any tailored internal privacy training Providers make available to their Personnel. Where required, the Provider must supplement the Department's privacy training module with its own additional privacy training.

6.13.1 Privacy Training Module

The Department's Information Exchange and Privacy Training Module explains the key concepts under the *Privacy Act 1988* and the APPs which govern how personal information is collected, used, disclosed, and stored.

The training module is mandatory and is essential to ensure that Personnel have a common understanding of this Chapter, the APPs, and the Social Security Law, including key processes that help manage potential risks. The completion of mandatory training assists Providers to meet legislative and regulatory requirements but is not sufficient to meet those requirements.

Privacy resources are also published on the Provider Portal for Personnel to access.

Providers should ensure their internal privacy practices, policies and procedures are proactively reviewed, compliant with new laws or updated information handling practices and responsive to new privacy risks.

6.13.2 Staff Compliance

Providers must monitor and annually self-audit Staff completion of privacy training, including the Department's mandatory Privacy training module. The Department may request details of a Provider's self-audit at any time or may conduct its own audit of a Provider's compliance with the requirements in this Chapter.

Where privacy training is undertaken outside of the Department's Learning Centre, the Provider must retain Records of privacy training undertaken by their Staff and must make this available to the Department on request.

It is also recommended that Providers put in place their own processes to audit the compliance of their Staff with privacy obligations more generally.



Chapter 7: External Systems Assurance Framework

7.1 Chapter Overview

This Chapter provides guidance for Providers on the External Systems Assurance Framework (ESAF) in relation to:

- meeting the Department's security and accreditation requirements
- obtaining accreditation, and
- maintaining accreditation for the duration of their Deed.

Providers can access Sensitive Information via the Department's IT Systems. This level of access requires appropriate levels of security.

Under the Government's Protective Security Policy Framework (PSPF), the Department of Employment and Workplace Relations (DEWR) is responsible for the protection of data entrusted in its systems and is accountable for ensuring contracted organisations and systems used in the delivery of employment services comply with relevant PSPF requirements. DEWR gives effect to these obligations, in part, through the ESAF. The Department works with DEWR to ensure that all Providers comply with requirements of the ESAF. Further information on the PSPF is available at protectivesecurity.gov.au.

DEWR, as the accrediting authority, uses the ESAF to determine that Providers and their External IT appropriately manage the level of risk to the security of information they hold. The ESAF sets out DEWR's accreditation of External IT Systems using a RFFR approach. As part of the ESAF, RFFR provides a tailored assurance approach to inform DEWR's decision. The RFFR approach closely follows the ISO 27001 international standard that sets out the requirements for an Information Security Management System (ISMS).

Providers are required to undertake the accreditation process and be accredited to demonstrate their ability to meet the Department's requirements for Provider information security in the manner and within the timeframes specified in this Chapter. Providers accredited under the ESAF must maintain their accreditation for the duration of their Deed with the Department, or the period they retain access to Personal Information collected during delivery of employment services (whichever is later).

If a Provider does not obtain accreditation or reaccreditation within the timeframes specified in the ESAF, including the RFFR, or their Deed, the Provider must immediately cease using, and ensure that any relevant Subcontractor ceases using, the relevant Provider IT System.

7.2 External Systems Assurance Framework

The ESAF provides assurance that the risks to the Department's IT Systems and data, information and Records stored outside of the Department's IT Systems environment are managed securely and appropriately. This is consistent with the whole of government Protective Security Policy Framework (PSPF).

As part of the PSPF, the Department, working alongside DEWR, is accountable for ensuring that all contracted Providers used in the delivery of its programs also comply with PSPF requirements.



The ESAF covers External IT Systems associated with:

- the delivery of the Services, including storage, processing or communication of data related to delivering the Services
- accessing the Department's IT Systems, and
- data, information and Records supporting the service.

The areas of assurance covered in the ESAF are Provider IT Systems and Third-Party Employment Systems (TPES).

7.2.1 Providers' IT Systems

Provider accreditation under the ESAF provides assurance that the Department's IT Systems and data are safeguarded when accessed by Providers and Subcontractors. The accreditation of Provider IT Systems provides assurance to the Department that sufficient security measures are in place to manage Provider and Subcontractor security risks.

7.2.2 Third Party Employment Systems (TPES)

TPES are any Third-Party IT Systems used in association with the delivery of the Services, whether or not that Third Party IT System Accesses the Department's IT Systems, and where that Third Party IT System:

- contains specific functionality or modules, or
- is used, in any way, for the analysis of Records relating to the Services, or any derivative thereof.

TPES are specialised and DEWR accredited systems that may interface with the Department's IT Systems and make employment industry-specific functionality available to licensed users.

Vendors of accredited TPES have demonstrated their implementation of an information security management system covering the TPES which meets RFFR requirements. The status of all existing accredited TPES is outlined on DEWR's [Digital Information Assurance and IT Security Compliance](#) website.

If a Provider uses a TPES, the Provider must ensure that they:

- have accessed the relevant TPES accreditation letter
- understand the scope of the TPES accreditation
- identify if the Provider's system configuration matches the accredited TPES configuration, and
- identify risks associated with use of unaccredited TPES functionality and implements appropriate mitigation strategies.

Providers wishing to use unaccredited software or services must assess risks, conduct their own evaluations, and ensure appropriate controls are in place.

Providers must obtain written approval from the Department to use or change a TPES.

(Deed reference: 42.12 - 42.14)



7.3 Right Fit For Risk approach

The RFFR approach includes requirements in relation to Provider accreditation based on the:

- **International Standard ISO/IEC 27001:2022** Information technology – Security techniques – Information security management systems – Requirements (ISO 27001) – the international standard outlining the core requirements of an Information Security Management System, and
- **Australian Government Information Security Manual (ISM)** – the Australian Government’s cyber security framework to protect systems and data from cyber threats.

The RFFR approach includes a requirement that Providers design and implement an Information Security Management System (**ISMS**) that is consistent with the requirements of ISO 27001. An ISMS is a systematic approach to managing business information so that it remains secure and available when staff need it. It secures people, premises, IT systems and information by applying a risk management process to information security.

The RFFR program extends ISO 27001 in 2 key areas:

- ISO 27001 requires organisations to consider the set of security controls presented in Annex A to the standard and identify which are applicable to mitigating their security risks. RFFR extends this requirement by asking Providers to also consider the set of security controls presented in the ISM that are relevant to securing OFFICIAL classified information, and
- The Department has identified core expectation areas that are particularly important to the security posture at all organisations. All Providers are expected to include security controls that support the core expectation areas under the RFFR when identifying applicable controls for inclusion in their ISMS.

7.4 Accreditation and maintenance of accreditation

DEWR is the accrediting authority for Providers. To accredit Providers, DEWR seeks assurance that the Provider has implemented an appropriate standard of security over their information and their IT environment. The accreditation process for each Provider depends on their size and risk profile.

To demonstrate that Provider IT Systems meet RFFR requirements, the Department requires Providers to follow the RFFR approach. The RFFR approach requires Providers to complete a set of milestones within a prescribed time period. At each milestone, Providers check in with DEWR to review progress, assess risk and provide guidance on meeting the RFFR requirements.

The milestones are designed to allow Providers to assess their organisation’s level of cyber security measures in place and implement any improvements identified at the same time as gaining a customised ISMS that conforms with ISO 27001.



7.5 Provider classification for accreditation

The RFFR approach classifies Providers into a category to obtain accreditation.

- Category 1: Providers delivering Services to 2,000 or more individuals per annum as a result of all of their Employment Services Deeds (including individuals serviced by Subcontractors), and
- Category 2: Providers delivering Services to fewer than 2,000 individuals per annum as a result of all of their Deeds (including individuals serviced by Subcontractors). This category includes two sub-categories referred to as "Category 2A" and "Category 2B" below.

When determining whether a Provider is in Category 2A or 2B, the Department will consider a range of risk factors including the:

- IT environment
- level of outsourcing
- Subcontracting arrangements
- organisational structure
- level of security maturity
- the extent of sensitive information held and level of access to Department's IT Systems, and
- other relevant factors.

The Department considers the number of individuals receiving Services from the Provider and any Subcontractors ("Caseload volume") in the aggregate across all Deeds. Should the Provider enter into new Deeds with the Commonwealth that alters the Caseload volume, DEWR will reassess their categorisation and may require the accreditation to be updated if the categorisation changes.

Each of the Provider categories is associated with its own assurance pathway under the RFFR approach.

DEWR will categorise a Provider based on their RFFR questionnaire submission (or equivalent) and additional information obtained through an interview with the Provider. Completion of this interview and categorisation activity marks Milestone 1 in the RFFR process.

Table 7-A provides guidance to Providers on the basis of accreditation and accreditation maintenance activities required for each category.

Table 7-A: Provider Classification

Accreditation	Category 1	Category 2A	Category 2B
Annual Case load	2,000 or more	Under 2,000	Under 2,000
Risk profile	Greater risk	Medium Risk	Low risk
Basis of accreditation	ISO 27001 conforming ISMS - independently certified	ISO 27001 conforming ISMS - self-assessed	Management Assertion Letter
Accreditation maintenance	Annual surveillance audit and triennial recertification	Annual self-assessment	Annual management assertion letter



Accreditation	Category 1	Category 2A	Category 2B
Milestones to complete	1, 2 and 3	1,2 and 3	1 and 3

7.6 Milestones for completing the accreditation process

7.6.1 Milestone 1

Respondents to relevant Requests for Tender (RFT) are required to submit a completed RFFR questionnaire to DEWR on how they use information and manage security. The completed questionnaire provides DEWR with information regarding the respondent's business, IT security posture, Subcontracting arrangements, and readiness to meet RFFR requirements.

Milestone 1 is initiated through the submission of a RFFR questionnaire required as part of a Provider's RFT response. DEWR will review the RFFR questionnaire, assess risk and provide guidance to Providers on completing subsequent Milestones of the RFFR accreditation process as relevant. On the execution of a Deed, the Department along with DEWR will engage with the Provider to discuss their IT security posture and next steps toward RFFR accreditation.

Table 7-B sets out the requirements for Milestone 1 for Providers who are already accredited or already in the process of being accredited.

Table 7-B: Requirements for the Milestone 1 process

Assessment method	Review of submitted RFFR questionnaire and discussion
Submission deliverables	RFFR questionnaire submitted by the Provider as part of their RFT response.
Key actions and outcomes	<p>The Provider and DEWR representatives will discuss the Provider's business, stakeholders, contractual obligations, information, systems and practices to assist the Provider to determine the scope of their Information Security Management System.</p> <p>Unaccredited Providers: DEWR will confirm the Provider's categorisation and the associated RFFR assurance requirements for completing Milestone 2 and 3. Providers intending to deliver Services to fewer than 2,000 individuals will review additional risk factors with DEWR to determine whether the Provider should be classified into Category 2A or 2B.</p> <p>Providers part way through an existing accreditation process: Existing Providers who are part way through an accreditation process for delivering Services under an existing Deed should take steps as advised in the purchasing documentation.</p> <p>Accredited Providers with new Deeds: DEWR will review the extent of changes to the Provider's scope of Services and determine if the Provider should be in a different category as a result of the new Deeds. In accordance with the terms of their accreditation, the Provider should consider whether their Information Security Management System requires review and update to ensure that people, locations, systems and information associated with Services under the new Deeds are appropriately secured; and notify the Department. If no significant changes have occurred, accredited Providers do not need to complete Milestones 2 and 3 and need only maintain their RFFR accreditation.</p>



Assessment method	Review of submitted RFFR questionnaire and discussion
Next steps	<p>For large organisations it is recommended Providers appoint a champion within the organisation to ensure compliance with the RFFR.</p> <p>Commence development of documentation required by the Provider's category (see Table 7-C below).</p> <p>Identify where existing security controls meet RFFR requirements, and where there are gaps requiring that additional controls be implemented.</p>
Due dates	Completed within one month of Deed execution by the Department.

7.6.2 Milestone 2

Milestone 2 requires Providers to demonstrate their ISMS has been designed to reflect RFFR requirements applicable for their Category (as advised at Milestone 1). Providers are required to demonstrate that appropriate security controls are planned to be implemented within the organisation through submission of required documentation.

The process for completing Milestone 2 depends on the Provider's category. This Milestone does not apply to Category 2B Providers who instead proceed directly to Milestone 3.

Reference guides, materials and templates to support Milestone 2 written submissions are available from DEWR's website. It is not mandatory to use DEWR's 's templates.

Table 7-C lists the requirements for Providers to achieve Milestone 2.

Table 7-C: Milestone 2 requirements

Requirement	Category 1 Provider	Category 2A Provider	Category 2B Provider
Submission deliverables	<ul style="list-style-type: none"> ISMS scope Statement of Applicability (SoA) reflecting RFFR requirements Independent assessor's Stage 1 report. 	<ul style="list-style-type: none"> ISMS scope SoA reflecting RFFR requirements ISMS Self-assessment report (conformance). 	Not applicable
Implementation status	Provider's ISMS is expected to substantially conform with ISO 27001 requirements; however applicable controls sourced from ISO 27001 Annex A and from the Australian Government Information Security Manual are not expected to be implemented at this stage.	Provider's ISMS is expected to substantially conform with ISO 27001 requirements; however applicable controls sourced from ISO 27001 Annex A and from the Australian Government Information Security Manual are not expected to be implemented at this stage.	Not applicable
Assessment method	Independently issued assessed by a JASANZ accredited ISO 27001 conformance assessment body.	Self-assessed by business owners.	Not applicable



Requirement	Category 1 Provider	Category 2A Provider	Category 2B Provider
Outcomes to progress to Milestone 3	DEWR acceptance of submission deliverables.	DEWR acceptance of submission deliverables.	Not applicable
Next steps	Implement the ISMS in accordance with its design.	Implement the ISMS in accordance with its design.	Not applicable
Due dates	To be completed within 3 months from the Deed Commencement Date.	To be completed within 3 months from the Deed Commencement Date.	Not applicable

7.6.3 Milestone 3

Milestone 3 emphasises the Provider’s progress to conforming with ISO 27001 and implementing the controls applicable to the organisation. While all applicable controls are important, priority should be on ensuring conformance with controls that support the RFFR core expectations.

If not fully implemented at the point of the Milestone 3 submission, Providers are required to inform DEWR of their expectation as to when each applicable control will be fully in place and when any remaining areas of non-conformance will be addressed.

Providers should be aware that applicable but unimplemented controls (and remaining areas of non-conformance) will impact the DEWR’s assessment of residual risk associated with the Provider, and DEWR’s decision to accredit the Provider. DEWR does not discourage any Category 2A and 2B Providers from seeking ISO 27001 certification as there may be significant perceived or actual benefits to other aspects of the Provider’s business.

Table 7-D lists the requirements for Providers to achieve Milestone 3.

Table 7-D: Milestone 3 requirements

Element	Category 1 Provider	Category 2A Provider	Category 2B Provider
Submission deliverables	<ul style="list-style-type: none"> Updated Scope document describing any changes to the Provider’s operating environment Updated SoA identifying the current implementation status of applicable controls, and the applicability decision for new or changed controls published since the SoA’s last review Independent assessor’s “Stage 2” report. This can be either an ISO27001 or DEWR ISMS Scheme report. RFFR does not require a Provider to have both audits completed 	<ul style="list-style-type: none"> Updated SoA identifying the current implementation status of applicable controls, and the applicability decision for new or changed controls published since the SoA’s last review ISMS self-assessment report (implementation) 	Management Assertion Letter



Element	Category 1 Provider	Category 2A Provider	Category 2B Provider
	<ul style="list-style-type: none"> ISO 27001 or DEWR ISMS Certificate 		
Implementation status	Provider's ISMS conforms with ISO 27001 and controls applicable to the organisation have been implemented	Controls supporting specific security objectives have been implemented	Controls supporting specific security objectives have been implemented
Assessment method	Independently assessed	Self-assessed	Self-assessed
Outcomes to complete process	<ul style="list-style-type: none"> DEWR acceptance of submission deliverables RFFR accreditation 	<ul style="list-style-type: none"> DEWR acceptance of submission deliverables RFFR accreditation 	<ul style="list-style-type: none"> DEWR acceptance of submission deliverables RFFR accreditation
Next steps	<ul style="list-style-type: none"> Address any remaining minor non-conformances Implement remaining applicable controls (if any) Monitor the ISMS 	Monitor performance of security controls	Monitor performance of security controls
Due dates	To be completed within 9 months from the Deed Commencement Date	To be completed within 9 months from the Deed Commencement Date	To be completed within 9 months from the Deed Commencement Date

7.7 Submission deliverables

7.7.1 Submission milestones

Table 7-E below provides a high-level description of the deliverables that need to be submitted to the Department as part of the accreditation process. DEWR does not require the use of any specific template, except for the RFFR questionnaire completed for Milestone 1 as part of the Provider's RFT response. Standard templates for each deliverable are available from DEWR and may be optionally used as a basis for working through the accreditation process.

Each of the submission deliverables in Table 7-E is described in more detail in Table 7-F.



Table 7-E: Provider Milestones Deliverables

Provider	Milestone 1	Milestone 2	Milestone 3
Category 1 Providers	<ul style="list-style-type: none"> RFFR questionnaire & Interview 	<ul style="list-style-type: none"> ISMS Scope SoA, and Independent assessor’s “Stage 1” report 	<ul style="list-style-type: none"> ISMS Scope SoA Independent assessor’s “Stage 2” report, and ISO 27001 certificate or DEWR ISMS certificate
Category 2A Providers	<ul style="list-style-type: none"> RFFR questionnaire & Interview 	<ul style="list-style-type: none"> ISMS Scope SoA, and ISMS Self-assessment report (conformance) 	<ul style="list-style-type: none"> ISMS Scope SoA, and ISMS Self-assessment report (implementation)
Category 2B Providers	<ul style="list-style-type: none"> RFFR questionnaire & Interview 	<ul style="list-style-type: none"> Not applicable 	<ul style="list-style-type: none"> Management Assertion Letter

7.7.2 Deliverable descriptions

Table 7-F below provides a detailed description of, and criteria for completing, each deliverable of the RFFR process.

Table 7-F: Deliverable descriptions

Submission Document	Description
RFFR questionnaire	Submitted with the Provider’s RFT response where required, the questionnaire seeks information regarding the Provider’s business, their IT security posture and their readiness to meet RFFR requirements. Discussing the completed questionnaire with the Department marks completion of Milestone 1 and confirms the Provider’s category.
ISMS scope document	The purpose of this document is to clearly define the boundaries of the ISMS to provide the Department with an understanding of the Provider’s business and context, in conformance with ISO 27001 Clause 4. It should also provide a high-level description of how the Provider intends to meet RFFR core expectation areas. A template scope document is available from the Department.
Statement of Applicability (SoA)	<p>The SoA demonstrates the Provider’s consideration of each of the security controls sourced from ISO 27001’s Annex A and ISM’s OFFICIAL security controls and the determination of which controls will form part of the Provider’s ISMS. It also communicates the rationale for determining that individual controls are “not applicable” to the Provider’s business.</p> <p>For applicable controls, the SoA should indicate relevant policies/procedures or other documentation demonstrating that the control has been included in the Provider’s business and should indicate the current implementation status of each applicable control.</p> <p>The SoA is a mandatory artefact required to conform with ISO 27001 Clause 6. An ISO to ISM controls mapping document is available from DEWR to assist with developing the SoA.</p>



Submission Document	Description
Independent assessor's "stage 1" report	For Category 1 Providers (or other Providers who see benefit in obtaining an industry certification). This is the first of 2 independent assessments required to achieve ISO 27001 or DEWR ISMS Scheme certification. Performed by a JASANZ registered certification assessment body, the stage 1 report verifies the extent to which the Provider's ISMS has been designed to conform with the requirements of ISO 27001 and identifies design gaps to be addressed prior to commencing the stage 2 assessment. Because RFFR requires a customised SoA it is critical that the report states that the assessment was performed over the ISMS as described by that customised SoA – with a clear report reference to the SoA by version/ date.
Independent assessor's "stage 2" report	For Category 1 Providers (or other Providers who see benefit in obtaining an industry certification). This is the second of 2 independent assessments required to achieve ISO 27001 or DEWR ISMS Scheme certification and is a key source of assurance that the Provider has implemented the controls identified as applicable in the SoA. Performed by a JASANZ registered certification assessment body, the stage 2 report validates that the implemented ISMS conforms with the requirements of ISO 27001 and that applicable controls are in place and operating. Because RFFR requires a customised SoA it is critical that the report states that the assessment was performed over the ISMS as described by that customised SoA – with a clear report reference to the SoA by version/ date - and that the report provides information regarding the status of both Annex A- and ISM-sourced applicable controls (particularly applicable controls that support RFFR core expectation areas - see section 6.9).
ISO 27001 certificate or DEWR ISMS Scheme certificate	Issued after the Provider has demonstrated plans to address any non-conformances identified in the stage 2 report and the independent assessor has recommended the Provider for certification. The DEWR ISMS Scheme certificate is an adaptation of the ISO 27001 certificate.
ISMS Self-Assessment report	For Category 2A Providers only, the self-assessment report is the Department's source of assurance that the ISMS described by the Provider's SoA has been designed (for Milestone 2) and implemented (for Milestone 3) in accordance with ISO 27001 and RFFR requirements. It is critical that the self-assessment report be signed off by a person/s with appropriate authority to make declarations on behalf of the Provider, that it attests to the Provider's ISMS conformance with ISO 27001 requirements, and (for Milestone 3) that it attest to the implementation status of controls identified as applicable in the Provider's SoA. A template self-assessment report is available from the Department.
Management Assertion Letter	For Category 2B Providers only, the Management Assertion Letter is the DEWR's source of assurance that the Provider represents minimal risk and has implemented security controls that respond to relevant security objectives. The letter covers a description of the Provider's systems and controls, attests that the description is accurate and that the described controls are appropriate to meet specific security objectives.



7.7.3 Considerations for accreditation commencement

Table 7-G provides guidance to Category 1, 2A and 2B Providers on areas of focus to consider before commencing the RFFR accreditation process.

Table 7-G: Considerations for accreditation commencement

Area	Description
Sponsor	Identify a sponsor within the organisation to support the RFFR certification process. The sponsor will help guide and support the accreditation process, including ensuring that appropriate resources are available to complete RFFR accreditation.
Scope	Determine the scope of the ISMS. Consider the organisational context and business activities performed at each Site, stakeholders and their needs, physical boundaries, legal and contractual requirements, and logical boundaries (systems and data). The scope should communicate key aspects of the Provider's business, the importance of security and state what the ISMS will be protecting.
Gap Analysis	Before the Milestone 2 submission, Providers should perform an initial review and gap assessment to identify areas of current conformance with ISO 27001 and areas requiring future focus. The gap assessment should also identify if the Provider already has some applicable controls in place and which require action to implement. As a management review of the ISMS, this assessment is itself a requirement of ISO 27001. Performing the gap assessment prior to Milestone 2 will ensure time to address non-conformances and to plan improvements before the Provider's final submission.
Certifying Assessment Body	For Category 1 Providers (or other Providers who see benefit in obtaining an industry certification), identify a suitable Certifying Assessment Body (CAB) to work with your organisation to provide the independent assessments required under the ISO 27001 requirements (see 7.7.4 below).

7.7.4 Certifying Assessment Bodies

To seek certification under the RFFR program, DEWR requires Category 1 Providers to be independently certified by a CAB/assessor. Providers are required to engage a CAB that is accredited or otherwise recognised by JASANZ to issue ISO 27001 or DEWR ISMS Scheme assessment reports and certificates in Australia.

JASANZ is the accreditation authority for CABs in Australia and New Zealand. A list of certifiers who can issue an ISO 27001 or DEWR ISMS Scheme assessment reports and certificates can be found at [JASANZ's website](#).

Category 2 Providers are not required to be independently certified by a CAB auditor. Category 2A Providers can self-assess and declare their conformance with ISO 27001 and the implementation status of applicable controls. Category 2B providers can provide a description of their business, systems and information and attest to their implementation of required security controls in the form of a management assertion letter.

7.8 Accreditation maintenance

During the lifespan of their Deed Providers are required to maintain their RFFR accreditation status through annual reporting (each Financial Year) and surveillance audits to ensure compliance to the standards (see Table 8-H below). Providers with an



existing accreditation will need to complete the annual and 3-yearly audits based on the dates when the accreditation was granted.

If, at any time during the accreditation maintenance period, a change to a Provider’s or Subcontractor’s circumstances alters the risk profile of the organisation, the Department will reassess the Provider’s accreditation status. This includes when the Provider or Subcontractor:

- enters a new Deed with the Department
- changes its Subcontracting arrangements (from one Subcontractor to another, or introduces a new Subcontractor)
- changes its Third-Party IT Vendors who are supporting their IT environments, and
- has a change in classification from Category 2 to Category 1.

The Provider must notify the DEWR within 5 Business Days of a change in circumstance.

ISM controls are regularly added and changed. Providers should regularly review these to consider whether the controls are applicable to their business and whether any of the controls should form part of their accredited ISMS. The SoA should be regularly revised to demonstrate the Provider's consideration of new or changed ISM controls. Where a new or changed control is determined to be applicable but has not been fully implemented by the time of the Provider's annual submission, Providers should ensure their SoA also includes details of their planned actions to address these matters and an expected completion date for each.

Table 7-H details the requirements for Providers to maintain their accreditation once accreditation has been granted. Note the timing of the annual and 3 yearly audits applies from the date of accreditation.

Table 7-H: Ongoing accreditation requirements

Accreditation type	Annually	Every 3 years
Certified ISMS (Category 1 Providers)	<ul style="list-style-type: none"> • Surveillance audit by CAB covering the Provider’s updated SoA 	<ul style="list-style-type: none"> • Recertification by CAB • Reaccreditation by DEWR
Self-assessed ISMS (Category 2A Providers)	<ul style="list-style-type: none"> • Self-assessment report (incl. description of changes since last report) covering the Provider’s updated SoA • DEWR determines whether need to upscale to a Certified ISMS 	<ul style="list-style-type: none"> • Self-assessment report • Reaccreditation by DEWR
Management attestation (Category 2B Providers)	<ul style="list-style-type: none"> • Annual attestation & description (incl. description of changes since last attestation) • DEWR determines whether need to upscale to a self-assessed ISMS 	<ul style="list-style-type: none"> • Attestation & description • Reaccreditation by DEWR

7.9 Core expectations of Providers under the RFFR

Providers must, as a minimum, implement and manage the following core expectations to maintain and enhance their security posture:

- Personnel security — implement security control measures including mature Personnel onboarding practices



- Physical security — implement appropriate physical security measures over IT equipment and storage media, and
- Essential Eight — identify a target level of maturity in each of the Essential Eight cyber security strategies published by the Australian Cyber Security Centre, develop a plan to achieve target maturity, and achieve a base level maturity in the first instance.

Providers should implement controls for:

- **Information Security Monitoring** — to manage vulnerabilities in their IT systems, and to manage changes to their IT systems
- **Incident management** — designed to detect and respond to cyber security incidents, to report incidents internally and to external stakeholders (including the Department) as appropriate, and to keep appropriate Records of security incidents. As a key element of security incident detection, Providers should implement controls to log security-related events occurring in their IT systems and to audit these logs on a regular basis, and
- **Restricted access controls** — to enable strong user identification and authentication practices for privileged accounts, user accounts, and service accounts.

Providers should implement security controls that are responsive to:

- **Specific Deed obligations** — such as data sovereignty
- **Specific or unique Provider security risks**, and
- **Continual improvement** — Commit to continual improvement as Cyber risks change and develop.

Providers are expected to demonstrate their responses to these core expectations through the submission of documentation at each RFFR milestone as detailed.

7.9.1 RFFR Core Expectations: Personnel security

As part of processes to bring new people into the organisation, Providers must:

- verify the competency of the individual by verifying qualifications, certifications and experience provided on their CV
- obtain satisfactory police check for the individual
- satisfactorily complete Working with Vulnerable People checks as required by individual states / territories
- confirm the individual has a valid right to work in Australia – a person who is not an Australian citizen must hold appropriate work entitlements
- verify that the individual has successfully completed initial and ongoing security awareness training programs with content and timing tailored to their role
- execute Deed which state that responsibilities for information security and non-disclosure requirements continue post termination, and
- implement higher levels of assurance for individuals that have privileged or administrative level access. The additional Personnel expectations include that individuals must be Australian citizens or permanent residents to give them sufficient connection with Australia and be willing and able to undertake a suitability background check.



7.9.2 RFFR Core Expectations: Physical security

Providers are required to implement physical security measures that minimise the risk of information and physical assets being:

- made inoperable or inaccessible, or
- accessed, used or removed without appropriate authorisation.

All Providers are expected to meet physical security expectations. Permanent facilities are to be commercial-grade facilities located within Australia. A facility is any physical space where business is performed to support the provision of government services. For example, a facility can be a building, a floor of a building or a designated space on the floor of a building. Providers allowing staff to work from home need to consider how the home environment can be configured to protect staff, program data and IT physical assets in the same manner as in the office environment. Personnel are to be aware of their environment when they transport or store their devices, and when they use mobile devices to access and communicate program data, especially in public areas. In such locations Personnel are to take extra care to ensure conversations are not overheard and data is not observed.

7.9.3 Essential Eight cyber security strategies

The Australian Cyber Security Centre (ACSC) has developed the Essential Eight strategies to mitigate cyber security threats.

Providers must determine a target maturity level for the Essential Eight cyber security strategies that reflects the organisation’s risk profile and develop plans to achieve target levels over time. The Department requires that Providers initially implement controls supporting the Essential Eight cyber security strategies to achieve Maturity Level One on the [ACSC’s published maturity model](#).

Detailed implementation guidance is also available from the [ACSC's website](#).

Table 7-I: Essential Eight cyber security strategies

Control	Description
Application Control	To control the execution of unauthorised software. This prevents unknown and potentially malicious programs executing in your environment.
Patch Applications	To remediate known security vulnerabilities in application software. Security vulnerabilities in applications can be used to execute malicious code. Using the latest version of applications and promptly applying patches when vulnerabilities have been identified will keep your environment robust.
Configure Microsoft Office macro settings	To block untrusted macros. Microsoft Office macros can be used to deliver and execute malicious code. This strategy will only allow macros from trusted locations with limited write access, or those digitally signed with a trusted certificate, to run.
Application Hardening	To protect against vulnerable functionality. Flash, ads and Java on the internet are popular ways to deliver and execute malicious code. This strategy requires the removal of unneeded features in Microsoft Office, web browsers and PDF viewers.



Control	Description
Restrict Administrative Privileges	to limit powerful access to systems. The access required by administrator accounts means they hold the keys to your IT kingdom. When compromised, adversaries use these accounts to gain full access to information and systems and move around Provider networks. Reduce this risk by minimising the number of these accounts and the level of privileges assigned to each account. Do not allow these accounts to be used to read email or web browsing.
Patch Operating Systems	to remediate known security vulnerabilities. Security vulnerabilities in operating systems can be used to further the compromise of systems. Do not use unsupported versions. Using the latest version of operating systems and promptly applying patches when vulnerabilities have been identified will limit the extent of cyber security incidents.
Multi-Factor Authentication	to protect against user accounts being inappropriately accessed. Stronger user authentication makes it harder for adversaries to access information and systems. This is particularly important when users perform higher risk activities such as gaining access remotely, performing administrative functions or when accessing sensitive data. Providers should note that multiple password challenges in series do not constitute multi-factor authentication (MFA) – MFA requires a combination of 2 or more factors made up of secret information (such as an ID/password combination); data uniquely bound to a physical device (such as an authenticator app on a registered smartphone or a one-time SMS code) and data uniquely bound to a physical person (a biometric measure such as facial recognition or a fingerprint).
Regular Backups	to maintain the availability of critical data and systems. This strategy assists with accessing information following a cyber security incident. Backups of data, software and configuration settings, stored disconnected from your main environment, can be used to recover from an incident. Regular testing of backups ensure it can be recovered and that all critical data is covered by the backup regimen.

7.10 General requirements

7.10.1 Security Contact

Providers are required to nominate one or more Security Contact officers who will act as point of contact during the term of their Deed. Providers are required to ensure that the contact information for Security Contact officers remains current and if there is a relevant change of staff that Providers update the Department within 5 Business Days of the change.

7.10.2 Subcontractor and Third-Party IT Vendor requirements

Providers are responsible for ensuring that any Subcontractors used in the provision of the Services and any Third-Party IT Vendors supporting the Provider's Services also comply with the security, privacy and data sovereignty requirements of their Deed.

The Provider must:

- ensure that its Subcontractors successfully complete the required Personnel vetting processes, and bear any costs associated with doing so, and



- ensure that its Subcontractors and its Third-Party IT Vendors are aware of, and comply with, the same security requirements that are placed on the Provider by the Department. This includes consideration and implementation of ISM OFFICIAL controls that are relevant to the scope of services provided by the Subcontractor or Third-Party IT service provider.

7.10.3 Access and information security assurance for External IT Systems

Providers (including any Subcontractors) who use an External IT System in association with the delivery of the Services must ensure that any External IT System used:

- does not breach Deed requirements relating to security, privacy and data sovereignty
- meets the relevant requirements of the ESAF
- does not introduce or permit the introduction of malicious code into the Department's IT Systems
- has secure logons for each operator such that each operator's logon is uniquely identifiable to the Department and entries are traceable, and have date and time stamps
- does not default answers to questions or input fields where the Department's IT Systems has no default setting, and
- is not used to access the Department's IT Systems without the Department's written approval.

7.10.4 Cloud Services Providers

In November 2021, the Digital Transformation Agency (DTA) released the Hosting Certification Framework. This Framework states that all information defined as government information must be hosted with the appropriate level of privacy, sovereignty and security controls.

The DTA maintains a list of [Certified Cloud Hosting Services](#). DEWR will provide advice to Providers on what this will mean towards achieving RFFR accreditation. However, it is important to note that Providers remain responsible for protecting the confidentiality, integrity, and availability of data through their own assurance and risk management activities.

7.10.5 Request for extensions to meet RFFR accreditation requirements

Providers may request an extension to meet accreditation requirements if they cannot submit their documentation on time due to reasons outside of their control. Best practice is for Providers to communicate in advance with DEWR about any impacts that may affect their ability to achieve their requirements. To support the Department's decision for extension requests, Providers must, at a minimum, provide the following:

- reason behind the request, and
- timeframes requested.

If the Provider requesting an extension is solely an Inclusive Employment Australia Provider, the Department will make the decision. If the Provider requesting an extension



is an Inclusive Employment Australia Provider, as well as a Provider of Other Employment Services such as Workforce Australia, the Department will work with DEWR to arrive at a joint decision on the request.

7.10.6 Breaches of security requirements under the Inclusive Employment Australia Deed

Where the Department considers the Provider has breached the security requirements of the Deed, or there is a risk of such a Breach, the Department may immediately take any action specified in clause 42 of the Deed, such as immediately suspending access, or requiring the Provider to cease all access, to the Department's IT Systems.

All Breaches will be handled by the Department and may utilise information from DEWR to assist with taking any relevant actions. DEWR is only the accrediting authority and will not be directly involved in resolving Breaches under the Inclusive Employment Australia Deed.

