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
Version 1.2	Published on: 4 September 2026	Effective from: 1 October 2026

In this version of the Guidelines, information has been added about the Inclusive Employment Australia Performance Framework, including:

- Glossary – added definitions of 'Australian Privacy Principle', 'Compliance Improvement Plan', 'Incident', 'Job Plan', 'Personal Information', 'Performance Improvement Plan', 'Protected Information' 'Re-engagement Appointment', and 'Sensitive Information'.
- Chapter 2: Provider Capability and Capacity
  - clarified Small Business eligibility for the Capacity Building Fund including expanded eligibility for Group Respondent Members and Material Subcontractors (section 2.7.2)
  - updated Documentary Evidence for reimbursement claims (s2.7.5).
- Chapter 4: Provider Performance Framework
  - added information about KPIs 1 and 2 (section 4.2.2)
  - advised a Performance Improvement Plan is required after two consecutive ratings of 'Improvement Required' instead of three (section 4.3.3)
  - added advice about the Inclusive Employment Australia Performance Guide (under Supporting Documents and at section 4.3.3).
- Chapter 6: Privacy
  - added information about collection and use of a Participant's Personal Information, including through Public Interest Certificates (6.9.2, 6.9.3).
- Chapter 7: External Systems Assurance Framework
  - added assurance category
  - refined the RFFR accreditation deliverables for providers
  - clarified the accreditation revocation process in the event a provider is unable to demonstrate ongoing compliance
  - added information about re-accreditation (out of cycle) and re-categorisation.

Contents

Inclusive Employment Australia Guidelines 0

Contents 2

Guideline Interpretation and Glossary 5

Reading notes 5

Related information 5

Glossary 5

Chapter 1: Operational Requirements 8

1.1 Chapter Overview 8

1.2 Inclusive Employment Australia Branding 8

1.3 Minimum Site requirements 8

1.4 Recipient Created Tax Invoices 9

1.5 Fraud and Corruption responsibilities 9

1.6 Dispute Resolution 10

1.7 Media enquiries 11

Chapter 2: Provider Capability and Capacity 12

2.1 Chapter Overview 12

2.2 Caseload 12

2.3 Collaboration with other Providers and community organisations 12

2.4 Staffing requirements 14

2.5 Provider staff training 15

2.6 Business continuity requirements 17

2.7 Capacity Building Fund 17

Chapter 3: Provider Servicing Standards 22

3.1 Chapter Overview 22

3.2 Code of Conduct and Service Guarantee 22

3.3 National Standards for Disability Services 23

3.4 Commonwealth Child Safety Framework 25

3.5 Customer Feedback Register 26

3.6 Complaint processes 26

Chapter 4: Provider Performance 29

4.1 Purpose and scope 29

4.2 Deed KPIs and alignment to the Performance Framework 29

4.3 Performance monitoring and regular assessments 30
4.4 Formal Performance assessments and management actions 30
4.5 Performance ratings and reporting 31
4.6 Compliance, assurance and service quality 31
Chapter 5: Record Management Instructions 32
5.1 Chapter Overview 32
5.2 Records Framework 32
5.3 Management of Records 33
5.4 Movement of Records 37
5.5 Transfer of Records 37
5.6 Data Migration 38
5.7 Breaches and Inappropriate Handling of Records 39
5.8 Retention of Records 39
5.9 Destruction of Records 40
Chapter 6: Privacy 43
6.1 Chapter Overview 43
6.2 Where to find your obligations 43
6.3 APP 3 and 5: Collection of solicited personal information 45
6.4 APP 4: Dealing with unsolicited Personal Information 51
6.5 APP 6: Use and Disclosure of Personal Information 51
6.6 APP 7: Direct marketing 53
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
6.9 Use and disclosure of Protected Information under Social Security Law 55
6.10 Privacy Incidents and the Notifiable Data Breaches Scheme 57
6.11 Privacy Complaints 57
6.12 Referring individuals to the Department in relation to privacy matters 58
6.13 Awareness and Training Expectations 58
Chapter 7: External Systems Assurance Framework 60
7.1 Chapter Overview 60
7.2 External Systems Assurance Framework 60
7.3 Right Fit for Risk 64
7.4 Reporting Requirements 70

7.5 Other Accreditation events 71
7.6 Glossary 73

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* (Cth)
- National Standards for Disability Services
- *Freedom of Information Act 1982* (Cth)
- *Privacy Act 1988* (Cth)
- *Archives Act 1983* (Cth)

Glossary

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

To the extent there are discrepancies between the below definitions and the legislation they come from (referenced below the definition), the current version of the definition contained in the legislation will be taken to be the correct definition.

Australian Privacy Principle or **APP** has the same meaning as section 6 of the *Privacy Act 1988* (Cth).

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.

Compliance Improvement Plans or **CIPs** are strategic plans developed by Providers to improve compliance with the Deed.

Incident means:

- an unplanned, accidental or deliberate event or happening resulting in personal injury (physical or mental), illness or damage to equipment, property, plant, site or building
- an event or happening that had the potential to result in personal injury (physical or mental), illness or damage to equipment, property, plant, site or building, or

- unacceptable or hostile behaviour that could result in legal proceedings or potential personal injury (physical or mental), illness or damage to equipment, property, plant, site or building.

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.

Job Plan means the employment pathway plan which a Participant (Mutual Obligation) must enter into with their Provider under Social Security Law, participation plan which a DSP Recipient (Compulsory Requirement) must enter into with their Provider under Social Security Law, or an agreement between the Provider and Participant that must be entered into by all other Participants in order to receive Services.

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 APPs.

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.

Personal Information means, as set out in Section 6 of the Privacy Act 1988 (Cth), information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not, and

(b) whether the information or opinion is recorded in a material form or not.

Protected Information means, as set out in Section 8 of the Disability Services and Inclusion Act 2023 (Cth), either of the following kinds of information:

(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 found an action by a person (other than the Commonwealth) for breach of a duty of confidence.

Re-engagement Appointment is a type of Appointment with the Provider for the purposes of Re-engagement of a Participant (Mutual Obligation) following an incident (or incidents) of non-compliance with their Mutual Obligation Requirements.

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

Sensitive Information means, as set out in Section 6 of the *Privacy Act 1988* (Cth):

(a) information or an opinion about an individual's:

(i) racial or ethnic origin

(ii) political opinions

(iii) membership of a political association

(iv) religious beliefs or affiliations

(v) philosophical beliefs

(vi) membership of a professional or trade association

(vii) membership of a trade union

(viii) sexual orientation or practices, or

(ix) criminal record

that is also personal information, or

(b) health information about an individual, or

(c) genetic information about an individual that is not otherwise health information, or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or

(e) biometric templates.

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. Participant confidentiality must be protected, as discussions may involve sensitive information about complex barriers to employment.
- Facilities and protocols must be in place to ensure security of 'Protected Information', as defined in the Disability Services and Inclusion Act 2023, 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 WHS 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. The Commonwealth Fraud and Corruption Control Framework 2024 is available via the Commonwealth Fraud Prevention Centre.

The Provider must take all reasonable steps to prevent, mitigate and detect Fraud and Corruption in accordance with the Commonwealth Fraud Control 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, and
- 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

Supporting Documents for this Chapter

- Capacity Building Fund – Fact Sheet
- Capacity Building Fund – Claim for Reimbursement Form

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): Clause 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): Clause 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 (TCF)	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 the Department of Employment and Workplace Relations (DEWR), the Department, Employers, National Panel of Assessors (NPA) Providers, the Complaints Resolution and Referral Service (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 Department's IT Systems, 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 their 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 Department's IT Systems and access to Participant's Personal and Protected Information.

Prior to Participant engagement

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

- Job Plans, and
- Targeted Compliance Framework (TCF).

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): Clause 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): Clause 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 paused
- arrange alternative servicing options for Participants, if appropriate
- reschedule Appointments or Activities, including contacting Employers, Activity 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 National Emergency Management Agency 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 to 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 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. The Department has absolute discretion over the decision to approve the reimbursement.

The following Sections set out which Providers are eligible for the Fund, categories of expenses that can be reimbursed under the Fund and how claims for reimbursement can be submitted.

2.7.2 Eligibility for the Fund

To be eligible for the Fund, the following criteria 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.

Organisations that are operating as Material Subcontractors, or Group Respondent Members, under an Inclusive Employment Australia Provider can also access capacity building supports (under Ancillary Payments) if they meet the definition of 'Small Business'.

- Under this arrangement, up to $150,000 (GST inclusive) will be available to each Provider that has an eligible Group Respondent Member or Material Subcontractor. The Provider must lodge the claim for reimbursement on behalf of the Group Respondent Member or Material Subcontractor.
- For the avoidance of doubt, the Provider can only claim up to $150,000 (GST inclusive) irrespective of how many eligible Group Respondent Members or Material Subcontractors it has.
- The Provider lodging the CBF claim on behalf of its eligible Group Respondent Member or Material Subcontractor agrees to pass on the approved CBF reimbursement in full to the Group Respondent Member or Material Subcontractor.

For ease of use, references to "Provider" in the following paragraphs include instances where the Provider is claiming on behalf of the eligible Group Respondent Member or Material Subcontractor. In these instances, the relevant documentary evidence must be in the name of the eligible Group Respondent Member or Material Subcontractor.

Small Business

Eligibility as a Small Business is based on the Provider's (or Group Respondent Member's or Material Subcontractor's) most recent financial statements at the time the Deed is executed.

The Provider must submit the financial statements it had, or its Group Respondent Member or Material Subcontractor had, at the time of Deed execution to demonstrate their (or its Group Respondent Member's or Material Subcontractor's) aggregated turnover was under $10 million.

(Deed Reference(s): Clause 167.6(c))

2.7.3 Eligible Expenditure

Eligible Expenditure for reimbursement categories are:

- achieving compliance with the NSDS
- obtaining 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 (7 August 2025). 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.

All claims for reimbursements must be submitted within 90 calendar days of payment of the eligible expense. For example, where an eligible expense was paid by the Provider on 1 March 2026, the Provider had until 30 May 2026 to lodge their application for CBF. If the claim for reimbursement was lodged after 30 May 2026, the expense will be deemed ineligible due to the 90-day rule.

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. However, 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 for delivering 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 is 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

- engaging a third party/IT company to assist with the accreditation process.

More information about RFFR can be found at Section **Error! Reference source not found.**.

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 (including any Deed extensions). All expenses submitted for reimbursement must be GST inclusive.

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

2.7.5 Submitting a Claim for Reimbursement form

All claims for reimbursement must be submitted to the Department within 90 calendar days of payment for the goods or services.

To claim reimbursement, Providers must complete the Claim for Reimbursement form, available on the Provider Portal, and email it together with all required documentary evidence and financial statements to DeedsAdvice@dss.gov.au for assessment.

For clarity, all expenses must, at minimum, include a Valid Tax Invoice which clearly details the expenses incurred, and a Receipt or Remittance that identifies the expenses have been paid in full by the Provider.

The table below outlines examples of documentary evidence required when seeking reimbursement for Eligible Expenditure.

Eligible Expenditure	Documentary Evidence / process
Financial support to achieve NSDS compliance or RFFR accreditation	• An email from DEWR advising RFFR accreditation has been achieved • NSDS Certificate of Compliance • Valid Tax Invoice and receipt demonstrating audit costs or timesheets for staff wages that related to attaining RFFR accreditation

Eligible Expenditure	Documentary Evidence / process

	• Evidence of payment from the Provider to a third-party supplier, such as:
	  ○ a record of transaction (bank statement or a record of transaction from the organisation's financial system)
	  ○ valid Tax Invoice with the receipt from the supplier
	  ○ a remittance advice, or
	  ○ other valid proof of payment.

All other eligible categories	• 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 claim for reimbursement

The Department will consider each claim for reimbursement based on eligibility criteria, Documentary Evidence and financial statements provided and email the Provider of its decision.

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 within the required timeframes. Major nonconformities must be resolved within 3 months and minor nonconformities 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 nonconformities.

  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 nonconformities 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 nonconformities identified in the audit**, and
  - Send a final copy of the Report to the Department.
- **Step 3**. **Undertake recertification audit**
  - Address any nonconformities identified in the audit
  - Finalise recertification, including resolving any nonconformities, 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 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 Commonwealth Child Safe Framework is relevant, the Department has included Child Safety clauses into the 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 1 November 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 Customer Resolution and Referral Service (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 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

Supporting Documents for this Chapter

- Inclusive Employment Australia Provider Performance Framework
- Inclusive Employment Australia Provider Performance Management Guide

4.1 Purpose and scope

The Department assesses Provider performance under the Inclusive Employment Australia Provider Performance Framework (Performance Framework), which provides a consistent, transparent and outcomes focused basis for understanding how Providers support Participants to prepare for, secure and maintain sustainable employment.

The Deed prescribes three Key Performance Indicators (KPIs): Quality, Effectiveness and Efficiency. These KPIs form the formal basis of all performance assessments while being interpreted and reported through the Performance Framework's operational structure.

This Chapter must be read with the Inclusive Employment Australia Performance Framework and the Inclusive Employment Australia Managing Provider Performance Guide.

These documents explain the Framework's methodology, measures and indicators and how the Department manages performance (including staged responses and formal assessments).

Further information about the Performance Framework is available on the Department's website.

4.2 Deed KPIs and alignment to the Performance Framework

The Performance Framework focuses on two core measures of success: Participant Experience and Helping People Find and Keep a Job. These measures directly align to the Deed's KPIs, which remain the formal basis for assessing Provider performance.

Deed KPI	Alignment to Performance Framework Measures of Performance	What This Means
KPI 1 – Quality	Participant Experience	This measures how Participants feel about the service they receive. It uses feedback from the Participant Experience and Capability Building Survey, including how satisfied people are and how well Providers communicate and support them.
KPI 2 – Effectiveness	Helping People to Find and Keep a Job	This looks at how well Providers help people get work and stay in work. It includes job placements and whether people stay in their jobs for 12, 26, or 52 weeks, as well as the quality of ongoing support.
KPI 3 – Efficiency	Not Assessed	

Notes on measures and indicators: Under the Performance Framework, Participant Experience is measured via survey-based indicators, including capability building and

service satisfaction and Helping People Find and Keep a Job is evidenced by indicators such as Employment Placement outcomes, Employment Duration at 12, 26 and 52 weeks, and Ongoing Support retention.

4.3 Performance monitoring and regular assessments

The Department monitors and assesses Provider performance on a regular and ongoing basis using data recorded in the Department's IT systems, program measures and indicators, internal assurance activities, NSDS compliance and audit outcomes, and feedback from Participants and Employers, alongside other relevant program information.

Performance monitoring includes regular checks that Providers maintain appropriate NSDS certification and continue to meet the service quality expectations outlined in the National Standards for Disability Services throughout the Deed Term.

Performance feedback may be provided at any time and may relate to continuous improvement, program expectations or matters relevant to the potential extension or non-extension of the Deed Term.

Regular performance assessments:

- May review performance at the overall Provider level, by Employment Service Area and by Site, including (as applicable) the performance of Group Respondent members and Subcontractors.
- May provide feedback through Performance Scorecards (see 4.5).

The Department may periodically review the Performance Framework to ensure fitness for purpose; any changes to indicators or measures do not alter the Deed KPIs.

4.4 Formal Performance assessments and management actions

During the Deed Term, the Department will undertake formal performance assessments of the Provider at times determined by the Department. Following a formal assessment, the Department may, without limitation of any rights under the Deed or at law, take action in accordance with clause 170 [Action about performance], having regard to the Provider's assessed performance.

The IEA Managing Provider Performance Guide sets out the Department's staged approach to managing underperformance, including early support, Performance Improvement Plans (PIPs) and market review, with escalation only where sustained underperformance continues after genuine support.

- **Stage 1** – A rating of Improvement Required for one quarter prompts targeted support discussions
- **Stage 2** – Performance Improvement Plan (PIP): Two consecutive quarters of Improvement Required triggers a formal PIP (usually up to three months to rectify, unless exceptional circumstances).
- **Stage 3** – Market review and further action: Failure to rectify following a PIP and/or a further quarter of Improvement Required may lead to a market share review and further action (up to discontinuation of services or contract termination by the Delegate, consistent with the Deed).

While performance ratings inform the market review process, they do not solely determine contract outcomes. In assessing a contract, the Department may also take into account relevant departmental data, payment verification findings, compliance activities, and any evidence of non-compliance with the National Standards for Disability Services (NSDS), alongside other relevant considerations.

The Department may also consider mitigating circumstances consistent with the Managing Provider Performance Guide (e.g., significant events beyond the Provider's control not already reflected in performance calculations) when determining whether action is required.

(Deed Reference(s): Clause 169, Clause 170 and Clause 171)

4.5 Performance ratings and reporting

Performance Scorecards communicate results to Providers and present performance against the Deed KPIs as interpreted through the two Framework measures - Participant Experience and Helping People Find and Keep a Job — at Provider and contract level where sufficient data is available. Providers receive ratings using standard definitions: Exceeds, Meets, Improvement Required, and Insufficient Data.

Performance for all KPIs is generally measured over a 12-month rolling period and shared quarterly.

Participant facing performance information (e.g., KPI ratings and explanatory descriptors) is published quarterly on the Department's website to support informed choice.

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.

4.6 Compliance, assurance and service quality

The Department reinforces performance expectations through robust contract management and assurance measures, including quarterly payment verification and annual reviews of service quality expectations aligned with the NSDS, in addition to ongoing monitoring of Deed compliance. Providers are required to maintain NSDS certification for the duration of the Deed.

Chapter 5: Record Management Instructions

Supporting Documents for this Chapter 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 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(s): Clause 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 1983* (Cth) 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* (Cth), 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 1988* (Cth) 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* (Cth) 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): Clause 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): Clause 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): Clause 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
- *Disability Services and Inclusion Act 2023*
- *Social Security (Administration) Act 1999*
- *Privacy Act 1988*
- *Australian Privacy Principles 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 as 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 (Cth) and the Australian Privacy Principles (the Privacy Law).

A Provider may also have other information handling obligations under the laws of States or Territories where it operates. It is the Provider's obligation under the Deed to make sure 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 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* (Cth) 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 Privacy Laws and requirements in these Guidelines, it is important for Providers to inform Participants about how they will handle 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 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 Section 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 Systems, where possible.

Please see Section 6.3.1 Participant consent requirements for information about the method of obtaining and recording Participant consent prior to them Commencing 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 informed 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 (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). 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 Section 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 Section 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.

A 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 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 the Participant's consent is current and checked for currency every 12 months or following a change in circumstances.

Before the first meeting or interview with the new or transferred Participant, the Provider may send the Participant a digital copy of the Direct Registration Form or Privacy Notification and Consent Form. This will give the Participant time to read and understand the contents of the form(s).

During the first meeting with the 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 withholding or withdrawing their consent may limit the services a Provider can provide a Participant with and may have implications for their 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 the Participant (or their Legal Guardian or authorised nominee) has provided valid consent for 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 1988 (Cth).

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 may still participate in the program and can be Commenced, even if they do not sign the Consent Form, provided that other requirements to be Commenced in the program have been met.

However, not signing the Consent Form may limit the services the Provider can offer the Participant, and may make it more difficult for the Participant to meet their Mutual Obligation Requirements.

Disclosure of the participant's information between the Department of Social Services, Services Australia, and the Department of Employment and Workforce Relations is part of being a participant of the Inclusive Employment Australia program. However, the Participant may withhold consent to the disclosure of their personal information to other third parties, such as:

- potential or actual employers;
- other Inclusive Employment Australia providers or other employment service providers;
- other allied health professionals or the National Panel of Assessors providers;
- education, training or other specialist supports organisations.

Providers must ensure that they take appropriate steps to manage the collection, use and disclosure of the participant's personal information where the participant has not signed the Consent Form, or withheld consent for disclosure to one or more third parties, or has revoked their consent.

Recording the Participant's consent

Providers must ensure 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, the Participant's Legal Guardian or Authorised 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 by 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.

The Privacy Act requires Providers to give Participants an APP 5 compliant Privacy Collection Notice. The *Privacy Notification and Consent Form* issued by the Department is an APP 5 compliant Privacy Collection Notice and hence, must be given to each Participant upon Commencement (noting that the Participant can still be Commenced even if they do not sign the Privacy Notification and Consent Form).

Providers 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 following a change in circumstances. Providers should make it clear to Participants that if they withhold or

withdraw their consent, this may ultimately limit the services a Provider can provide the Participant and may have implications for their mutual obligation requirements.

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 Legal Guardian or Authorised 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.

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 Systems as an appropriate comment.

Where consent is not provided or is withdrawn and no APP exception applies, the Provider cannot collect the individual's Sensitive Information. In these circumstances, Providers must explain to the individual they may still be required to participate in the program; however the lack of consent may limit the options and employment services the 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 skilled 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 under Social Security Law. If they are a Volunteer (Non-mutual obligation) 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 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 impractical 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 to the Department's IT Systems materials containing the Personal Information 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 Commonwealth, State or Territory 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 Systems. 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* (Cth) 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* (Cth).

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 Inclusive Employment Australia participant privacy and consent.

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).

* **Note:** 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 IT Systems 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 the Department's IT Systems 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 Assessors, or other qualified health and allied health professionals to undertake assessments or provide services as part of the program.

The National Panel of Assessors (NPA) 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 Progress Fees, 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* (Cth).

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 their Deed, Providers must consider whether the proposed marketing is consistent with the *Privacy Act 1988* (Cth). 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* (Cth) 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* (Cth) 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 under Social Security Law

Information about a participant who has Mutual Obligation Requirements, is "Protected Information" under the Social Security Act.

Under Social Security Law, a Provider's Personnel may obtain, record, use and disclose Protected Information for the purposes of efficient and effective delivery of work-related services to Participants. 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 the Department's IT Systems about a Participant who has Mutual Obligation Requirements is Protected Information.

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 to the Participant, insofar as it relates to their Mutual Obligation Requirements.

Providers can also make a record of, use, and disclose a Participant's Protected Information where that Participant provides express or implied consent to that use or disclosure. This may be helpful where a Provider wishes to assist or support the Participant 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.

The DES Class PIC, issued under the *Social Security (Administration) Act 1999* and paragraph 28(5)(a) of the *Disability Services Act 1986* (Cth), enables disclosure by providers of Protected Information in specified circumstances as outlined in the DES Class PIC.

Providers must complete the *Class PIC - Release of Protected Information Form* on the Provider Portal when a disclosure has occurred in reliance of the DES Class PIC.

For other circumstances not covered by the DES Class PIC, a specific PIC will need to be requested by the Provider from the Department by sending a *Specific PIC Request Form* to the Account Management Team. The Department will only issue a specific PIC in accordance with the PIC Guidelines. Each request for a specific PIC will be assessed on a case-by-case basis.

6.9.4 Direct Registration Participants

Providers must handle the information of Direct Registration Participants in the same way as those of Participants with Mutual Obligation or Compulsory Requirements. This means that Providers can only disclose their information in circumstances where the Social Security Law (including PICs) would authorise such a disclosure.

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* (Cth) 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 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 IT Systems.

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

Under the Government's Protective Security Policy Framework (PSPF), the Department is responsible for ensuring contracted organisations and systems used in the delivery of employment services comply with relevant PSPF requirements.

The External Systems Assurance Framework (ESAF), which is administered by the Department of Employment and Workplace Relations (DEWR), is the mechanism under which the Department gains assurance over External IT Systems, and provides information for Providers in relation to:

- the security and assurance requirements that Providers must meet under the ESAF, and
- how Providers must meet these security and assurance requirements, including through achieving and maintaining Right Fit For Risk (RFFR) Accreditation for any Provider IT System, and in relation to Third Party IT accreditation.

A Provider's failure to comply with any applicable ESAF requirement (including any requirement in relation to timeframes) may constitute a breach of the Deed, and the Department may take action against the Provider in relation to the breach in accordance with the Deed.

7.2 External Systems Assurance Framework

The objective of the ESAF is to ensure that any External IT Systems and supporting processes used in the delivery of Services are compliant with Australian Government security and privacy requirements.

The ESAF provides a structured assurance framework for all External IT Systems used by Providers or any Subcontractors that:

- support the delivery of Services, or
- are used to Access the Department's IT Systems.

This includes Provider IT Systems and any Third Party IT.

The use of External IT Systems in association with the delivery of Services or to Access the Department's IT Systems introduces security risks that must be actively managed. Responsibility for managing these risks is shared between the Department, Providers and Third Party IT Vendors. This shared approach ensures that appropriate safeguards are in place to protect relevant information throughout the term of the Deed.

Developed in alignment with the Protective Security Policy Framework (PSPF), the ESAF ensures the Right Fit For Risk (RFFR) accreditation approach reflects whole-of-government security requirements, as well as relevant legislative and regulatory obligations.

The ESAF is reviewed annually by DEWR to ensure continued alignment with whole-of-government obligations, evolving regulatory requirements, and DEWR's strategic objectives. These reviews inform updates to ESAF requirements.

7.2.1 Templates and other resources

Providers must ensure that all information provided to DEWR for the purposes of meeting ESAF requirements is true, accurate and complete, and reflects the Provider's current security posture.

To assist Providers in achieving and maintaining RFFR Accreditation, DEWR publishes templates and other resources on its website. Providers must use the latest version of templates relevant to their assigned Assurance Category when submitting Deliverables required for the purposes of meeting ESAF requirements.

DEWR may publish updates to these templates and other resources to reflect changes to DEWR's and whole-of-government security requirements. If DEWR issues a new version of a template less than three (3) months before a Provider's Deliverables are due, the Provider may choose to use either the previous version or the updated version.

7.2.2 RFFR Core Expectations

Under the ESAF, each Provider is assigned to one of four Assurance Categories based on the risk profile of their organisation. Providers must comply with all RFFR Core Expectations set out in the ESAF, in addition to any category-specific requirements that apply to them.

Personnel Security

Providers must ensure that prior to employing or engaging any individual to support the delivery of Services, they:

- verify the individual's identity through positive identification procedures,
- obtain a satisfactory police check for the individual,
- ensure that the individual:
  - is an Australian citizen, or
  - where the individual is not an Australian citizen or Australian permanent resident, that they hold a valid visa with the appropriate right to work, and
- ensure, as a condition of their employment or engagement, that:
  - the individual is subject to information security and non-disclosure obligations that meet the requirements under the relevant Deed, and
  - such obligations continue to apply to the individual after their employment ends.

Subcontractors

To the extent that subcontracting is permitted under the relevant Deed, Providers must ensure that any Subcontractors comply with all security, privacy and data sovereignty obligations set out in the relevant Deed.

Physical Security

Providers must implement physical security measures at Facilities that minimise the risk of information and physical assets being:

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

Cyber Security

Providers must establish, implement, and maintain cyber security measures proportionate to their risk profile, to minimise the risk of the Department's information and supporting systems (including External IT Systems) being:

- compromised, altered, or disclosed without authorisation, or
- made unavailable or otherwise unable to support the delivery of the Services.

The cyber security measures must include measures to:

- identify and manage cyber security risks, including risks arising from the provision of Services under the Deed,
- define security governance, roles, and responsibilities for managing cyber security within the Provider's organisation,
- implement and maintain security controls that are appropriate to the Provider's assigned Assurance Category and applicable to the Provider's IT and operating environment,
- detect, respond to, and recover from cyber security incidents in a timely manner, to ensure early identification and response and support business continuity and the continued provision of Services;
- monitor system security and identify and implement any changes necessary to ensure the ongoing effectiveness of the Provider's security program, and
- continually review and improve cyber security measures to remain effective against evolving threats.

7.2.3 External IT Systems

An 'External IT System' means any information technology system or service (including any cloud platform), other than the Department's IT Systems, used by the Provider or any Subcontractor in association with the delivery of the Services or to Access the Department's IT Systems. 'External IT System' includes a Provider IT System and any Third Party IT.

Providers must ensure that any External IT System used in association with the delivery of the Services or to Access the Department's IT Systems:

- complies with all Deed requirements, including requirements relating to privacy and data sovereignty, and
- meets the relevant requirements of the ESAF.

Where under the Deed the Department requires that the Department's IT Systems are used to collect or store Participant information, or to perform certain tasks in the delivery of Services, Providers must not use any External IT System for that purpose, even if that External IT System meets the requirements of the ESAF.

Third Party IT

'Third Party IT' means any:

- information technology system (including any cloud platform) developed and managed, or
- information technology service provided,

by a Third Party IT Vendor and used by the Provider or any Subcontractor in association with the delivery of the Services or to Access the Department's IT Systems. 'Third Party

IT' includes a Third Party Employment and Skills (TPES) System and a Third Party Supplementary IT System (TPSITS).

Providers must ensure that their Accreditation Deliverables describe all Third Party IT used by the Provider or any Subcontractor in association with the delivery of the Services or to Access the Department's IT Systems.

TPES System

A TPES System is any Third Party IT used in association with the delivery of the Services, whether or not that Third Party IT Accesses the Department's IT Systems, and where that Third Party IT contains program specific functionality or modules.

An accredited TPES System may be used for the analysis of Records relating to the Services or any derivative thereof.

The Provider must not use a TPES System to Access the Department's IT Systems or electronic Records relating to the Services unless it has been accredited by DEWR in accordance with a Third Party IT Vendor Deed. Before using a TPES System, the Provider must:

- ensure that the relevant Third Party IT Vendor has entered into a current Third Party IT Vendor Deed with DEWR in relation to the TPES System,
- confirm that the TPES System is currently included in the list of accredited TPES Systems published on DEWR's website,
- review the relevant TPES System's RFFR accreditation report, including the scope of the TPES System's RFFR accreditation and description of shared responsibilities, and
- implement any controls and/or system configuration requirements specified in the relevant TPES System's RFFR accreditation report as 'customer responsibilities'.

DEWR's accreditation of a TPES System provides assurance that the TPES System meets DEWR's security requirements. However, Providers remain responsible for ensuring that any TPES System is configured and used in a way that effectively mitigates their own information security risks. DEWR does not warrant that any TPES System that is accredited in accordance with a Third Party IT Vendor Deed is fit for its intended use or for a Provider's specific business processes, or is free from error or security weaknesses.

Before using an accredited TPES System, the Provider must ensure that the TPES System is identified, and its use clearly described, within the Provider's Accreditation Deliverables and where relevant, its Updated Deliverables.

TPSITS

A TPSITS is any Third Party IT used in association with the delivery of the Services, where that Third Party IT:

- does not Access the Department's IT Systems, and
- does not contain program specific functionality or modules.

A TPSITS may be used for the analysis of Records relating to the Services or any derivative thereof.

A TPSITS is not accredited by DEWR for the purposes of the ESAF. However, before using a TPSITS, the Provider must ensure that the TPSITS:

- is included within the scope of the Provider's RFFR Accreditation and clearly described within their Accreditation Deliverables, and

- complies with all ESAF requirements applicable to the Provider's assigned Assurance Category.

7.3 Right Fit for Risk

DEWR's RFFR assurance approach operationalises the ESAF by defining the processes through which DEWR obtains assurance over External IT Systems. It applies a risk-based methodology to ensure requirements are proportionate to the DEWR's risk exposure and establishes the Assurance Lifecycle through which Providers achieve and maintain RFFR Accreditation.

Assurance Lifecycle

DEWR is responsible for granting RFFR Accreditation to Providers. To obtain RFFR Accreditation, Providers must demonstrate to DEWR's satisfaction that they have implemented reasonable and appropriate security controls to support the secure delivery of the Services and protect the Department's information.

The Assurance Lifecycle sets out the stages through which assurance is established and maintained under the RFFR accreditation approach. It provides a structured approach to managing assurance activities throughout the Term of the Deed.

Providers must achieve the requirements of each stage of the Assurance Lifecycle within the timeline specified below and to DEWR's satisfaction.

Table A – Assurance Lifecycle

Assurance Lifecycle stage	Timeline
Categorisation	The Provider must complete the Categorisation stage within **one month** of the Deed commencement Date.
Initial Assessment	The Provider must submit the Initial Assessment Deliverables within **two months** of the Deed commencement Date. The Provider must complete the Initial Assessment stage within **three months** of the Deed commencement Date.
Accreditation	The Provider must submit the Accreditation Deliverables at least **six weeks** before the Provider is required to obtain RFFR Accreditation. The Provider must obtain RFFR Accreditation within **nine months** of the relevant Deed commencement Date.
Accreditation Maintenance	The Provider must submit Updated Deliverables at least **six weeks** before the Provider is required to complete the Accreditation Maintenance stage. The Provider must complete the Accreditation Maintenance stage every **12 months** from the date that RFFR Accreditation was obtained, other than every third year when the Provider must instead complete the Reaccreditation stage.
Reaccreditation	The Provider must submit Updated Deliverables at least **six weeks** before the Provider is required to complete the Reaccreditation stage. The Provider must complete the Reaccreditation stage every **three years** from the date that RFFR Accreditation was obtained.

Categorisation

Categorisation is the first stage of the Assurance Lifecycle and is used by DEWR to determine the Provider's Assurance Category. The Assurance Category that is assigned by DEWR to the Provider in the Categorisation stage will determine the level of assurance that is required for the Provider to achieve RFFR Accreditation.

The Provider must submit the Categorisation Deliverables and undertake the assurance activities required for the Categorisation stage, as set out in Table B, within **one month** of the Deed commencement Date.

Table B – Categorisation Deliverables and assurance activities

Deliverable/Activity	Description
Categorisation Questionnaire	The Provider must submit a Categorisation Questionnaire as part of their response to the relevant procurement or grant documentation.
Categorisation Meeting	The Provider must attend a Categorisation Meeting with DEWR for the purposes of: • validating the information provided by the Provider in the Categorisation Questionnaire, • enabling DEWR to understand the Provider's operating model and External IT System/s, and • discussing the RFFR accreditation approach, including key stages and timeframes, to assist in identifying the systems and processes that are within the scope of accreditation.
Outcome and next steps	DEWR will assess the information and Categorisation Deliverables provided by the Provider in the Categorisation Questionnaire and Categorisation Meeting and notify the Provider of their assigned Assurance Category and the associated assurance requirements.

In the Categorisation stage, the Provider is assigned one of four Assurance Categories (i.e. Category 1, Category 2, Category 3 or Category 4) by DEWR following an assessment of:

- the service delivery context, and
- the Provider's operating model.

Service delivery context refers to the nature of the Services delivered by the Provider, and the type and volume of information that the Provider is required to handle in delivering the Services.

Operating model refers to the Provider's organisational and technical characteristics that influence the complexity of the environment in which Services are delivered. Indicative relevant factors that DEWR will take into account include:

- system integrations and data flows,
- data storage arrangements,
- the complexity of the Provider's IT environment,
- organisational scale,
- supply chain involvement, and
- relevant historical security or privacy incidents.

These examples are provided for context and do not limit DEWR's ability to consider any additional factors that are relevant to the Provider's threat and risk profile as part of its assessment for the Categorisation stage.

Upon the completion of the Categorisation stage, DEWR will assign to the Provider the Assurance Category that best reflects the Provider's overall threat and risk profile. The four Assurance Categories represent graduated levels of assurance that scale according to different risk profiles. Higher categories correspond to environments that involve greater exposure to sensitive information or increased operating complexity, and lower categories apply to environments with limited data exposure or simpler operations.

Initial Assessment

The Initial Assessment stage involves an assessment by DEWR of the Provider's security posture against the requirements of their assigned Assurance Category.

The Initial Assessment stage considers:

- the context in which the Services are delivered,
- the implementation of applicable security controls, and
- any associated risk treatment plans.

The Initial Assessment stage enables DEWR to assess how the Provider will safeguard the Department's information and to determine the Provider's readiness to progress toward obtaining RFFR Accreditation.

The Provider must submit the Initial Assessment Deliverables required for the Initial Assessment stage in accordance with their assigned Assurance Category, as specified in Table C below, within **two months** of the Deed commencement Date. This timeframe is to allow DEWR to complete the Initial Assessment stage within **three months** of the Deed commencement Date.

Where DEWR determines that the submitted Initial Assessment Deliverables do not clearly demonstrate the Provider's security posture, DEWR may:

- request clarification from the Provider where information is missing, incorrect, or unclear, and
- in exceptional circumstances, consider limited adjustments to the Initial Assessment stage timeframe where DEWR determines that additional time is required for the Provider to address identified deficiencies.

DEWR will notify the Provider when it has successfully completed the Initial Assessment stage.

Table C – Initial Assessment Deliverables

Category	Deliverable	Description
Category 4	• Security Assessment Questionnaire (SAQ)	A Category 4 Provider must complete a SAQ outlining the Provider's current implementation of applicable security controls, including treatment plans for applicable controls not yet fully implemented.
Category 3	• Provider Security Plan (PSP) • PSP Annex	A Category 3 Provider must submit a completed: • PSP clearly defining the scope of the Services and security controls in place to safeguard the Department's information, and • PSP Annex with all applicable Category 3 controls addressed to reflect their current implementation, along with a treatment plan for applicable controls not yet fully implemented.

Category	Deliverable	Description
Category 2	• Provider Security Plan (PSP) • PSP Annex	A Category 2 Provider must submit a completed: • PSP clearly defining the scope of Services and security controls in place to safeguard the Department's information, and • PSP Annex with all applicable Category 2 controls addressed to reflect their current implementation, along with a treatment plan for applicable controls not yet fully implemented.
Category 1	• Provider Security Plan (PSP) • PSP Annex • ISO/IEC 27001 or DEWR ISMS Scheme Stage 1 Audit Report	A Category 1 Provider must submit: • a completed PSP clearly defining the scope of Services and security controls in place to safeguard the Administering Department's information, • a PSP Annex with all applicable Category 1 controls addressed to reflect their current implementation, along with a treatment plan for applicable controls not yet fully implemented, and • an ISO/IEC 27001 or DEWR ISMS Scheme Stage 1 Audit Report conducted by a JASANZ accredited certification body, validating the Provider's approach to implementing applicable controls within the PSP Annex.

Note: As part of DEWR's initial assessment of a TPES System for the purposes of its accreditation in accordance with a Third Party IT Vendor Deed, Third Party IT Vendors are required to submit to DEWR:

- a completed System Security Plan (SSP) clearly defining the scope of the TPES System and security controls in place to safeguard the Administering Department's information,
- a SSP Annex with all applicable controls addressed to reflect their current implementation, along with a treatment plan for applicable controls not yet fully implemented, and
- an ISO/IEC 27001 or DEWR ISMS Scheme Stage 1 Audit Report conducted by a JASANZ accredited certification body, validating the implementation of applicable controls within the SSP and SSP Annex.

Accreditation stage

The Provider must achieve RFFR Accreditation within **nine months** of the Deed commencement Date. The Provider must submit all required Accreditation Deliverables, as specified in Table D below, no later than **six weeks** prior to the deadline for achieving RFFR Accreditation.

If a Provider does not obtain RFFR Accreditation within nine months of the Deed commencement Date, the Provider must immediately cease using, and ensure that any relevant Subcontractor ceases using, the relevant Provider IT System.

DEWR will assess the Provider's security posture for RFFR Accreditation based on the Accreditation Deliverables submitted by the Provider, as specified in Table D. As part of this assessment, DEWR will evaluate the Provider's service delivery context, data lifecycle, operating model, and implementation of applicable security controls, including any associated risk treatment plans.

Where DEWR determines that the submitted Accreditation Deliverables do not clearly demonstrate the Provider's security posture, DEWR may at its absolute discretion:

- request clarification from the Provider where information is missing, incorrect, or unclear,
- request evidence from the Provider to confirm the implementation or effectiveness of security controls, and/or
- in exceptional circumstances, consider a limited adjustment to the Accreditation stage timeframe where DEWR determines additional time is required for the Provider to address identified deficiencies.

The Provider's RFFR Accreditation is achieved upon the Provider's successful completion of the Accreditation stage, as notified to the Provider by DEWR, following DEWR's assessment of, and formal acceptance of the residual risk associated with, the Provider's security posture.

A Provider's RFFR Accreditation remains valid for **three years** (unless it is revoked in accordance with the ESAF), at which time the Provider must have successfully completed the Reaccreditation stage in order to maintain its RFFR Accreditation status.

Table D – Accreditation Deliverables

Category	Deliverable	Description
Category 4	• Security Assessment Questionnaire (SAQ)	A Category 4 Provider must submit an updated and completed SAQ describing the current implementation of applicable security controls and any risk treatment plans or changes to the Provider's security posture since the Initial Assessment stage.
Category 3	• Provider Security Plan (PSP) • PSP Annex	A Category 3 Provider must submit an updated and completed PSP and PSP Annex clearly defining the scope of Services and security controls in place to safeguard the Administering Department's information.
Category 2	• Provider Security Plan (PSP) • PSP Annex	A Category 2 Provider must submit an updated and completed PSP and PSP Annex clearly defining the scope of Services and security controls in place to safeguard the Administering Department's information.
Category 1	• Provider Security Plan (PSP) • PSP Annex • ISO/IEC 27001 or DEWR ISMS Scheme Stage 2 Audit Report • ISO/IEC 27001 or DEWR ISMS Scheme Corrective Actions Plan • ISO/IEC 27001 or DEWR ISMS Scheme Certificate	A Category 1 Provider must submit: • an updated and completed PSP and PSP Annex clearly defining the scope of Services and security controls in place to safeguard the Administering Department's information, • an ISO/IEC 27001 or DEWR ISMS Scheme Stage 2 Audit Report conducted by a JASANZ accredited certification body, validating the Provider's approach to implementing applicable controls within the PSP Annex, • an ISO/IEC 27001 or DEWR ISMS Scheme Corrective Actions Plan (if applicable), and • an ISO/IEC 27001 or DEWR ISMS Scheme Certificate.

Note: As part of DEWR's assessment of the security posture of a TPES System for the purposes of its accreditation in accordance with a Third Party IT Vendor Deed, Third Party IT Vendors are required to submit to DEWR:

- an updated and completed System Security Plan (SSP) and SSP Annex clearly defining the scope of the TPES System and security controls in place to safeguard the Administering Department's information,
- an ISO/IEC 27001 or DEWR ISMS Scheme Stage 2 Audit Report conducted by a JASANZ accredited certification body, validating the implementing of applicable controls within the SSP and SSP Annex,
- an ISO/IEC 27001 or DEWR ISMS Scheme Corrective Actions Plan (if applicable), and
- an ISO/IEC 27001 or DEWR ISMS Scheme Certificate.

Accreditation Maintenance stage

The Accreditation Maintenance stage is an annual assurance activity that ensures the Provider's security posture remains appropriate for the secure delivery of Services and the protection of the Administering Department's information. This stage requires that any significant changes to the Provider's service delivery, operating model, supporting systems or data handling practices are accurately reflected in the Provider's Updated Deliverables.

The Accreditation Maintenance stage must be completed by the Provider every 12 months from the date of the RFFR Accreditation (the Accreditation Maintenance Date), other than every third year, when the Provider must instead complete the Reaccreditation stage.

At least **six weeks before** each Accreditation Maintenance Date, the Provider must submit to DEWR the Updated Deliverables. The Updated Deliverables must reflect the Provider's current operating environment and External IT Systems.

Where DEWR determines that the Updated Deliverables do not clearly demonstrate the Provider's security posture, DEWR may at its absolute discretion:

- request clarification from the Provider where information is missing, incorrect, or unclear,
- request evidence from the Provider to confirm the implementation or effectiveness of security controls, and/or
- in exceptional circumstances, consider a limited adjustment to the Accreditation Maintenance stage timeframe where DEWR determines additional time is required for the Provider to address identified deficiencies.

DEWR will notify the Provider once it has successfully completed the Accreditation Maintenance stage.

Reaccreditation stage

The Reaccreditation stage involves a full reassessment by DEWR of the Provider's security posture to confirm continued compliance with the ESAF requirements for the Provider's assigned Assurance Category, taking into account the Provider's RFFR accreditation history.

The Provider must successfully complete the Reaccreditation stage every third year from the date that the Provider obtained RFFR Accreditation (the Reaccreditation Date). Completion of the Reaccreditation stage ensures that the Provider's security posture remains aligned to whole-of-government requirements and Departmental priorities.

At least **six weeks before** the Reaccreditation Date, the Provider must submit to DEWR the Updated Deliverables. The Updated Deliverables must reflect the Provider's current operating environment and External IT Systems.

Where DEWR determines that the submitted Updated Deliverables do not clearly demonstrate the Provider's security posture, DEWR may at its absolute discretion:

- request clarification from the Provider where information is missing, incorrect, or unclear,
- request evidence from the Provider to confirm the implementation or effectiveness of security controls, and/or
- in exceptional circumstances, consider a limited adjustment to the Reaccreditation stage timeframe where DEWR determines additional time is required for the Provider to address identified deficiencies.

The Provider must successfully complete the Reaccreditation stage in order to maintain its RFFR Accreditation. DEWR will notify the Provider once it has successfully completed the Reaccreditation stage.

7.4 Reporting Requirements

Change of Circumstances

The Provider must notify their Departmental Account Management Team and DEWR of any change of circumstances that may alter the risk profile of their organisation by submitting a Change of Circumstance form within **5 Business Days** of a change of circumstance. Where applicable, this includes, but is not limited to, when the Provider:

- enters into a new Deed or terminates a Deed,
- changes its legal or organisational arrangements, including to its:
  - legal entity details (such as changes to its legal entity or business name(s)),
  - organisational or corporate structure (including subsidiaries or group member organisations), or
  - key Personnel or governance roles (such as Chief Executive Officer, Chief Information Security Officer or equivalent positions).
- changes its market share or the location(s) from which it delivers Services (including employment regions or sites),
- changes how it handles information, or the volume or sensitivity of information it handles,
- changes its subcontracting arrangements (from one Subcontractor to another, or introduces a new Subcontractor),
- changes its IT systems, infrastructure or online services,
- changes its Third-Party IT Vendors who are supporting its IT environments, and/or
- implements the use of AI technology in the delivery of Services.

DEWR will assess any change of circumstances notified by the Provider and determine whether the Provider is required to complete the Reaccreditation stage (out of cycle) or a reassessment of the Provider's Assurance Category is required.

In the event of a change of circumstances, the Provider must provide to DEWR any additional information within the timeframes requested by DEWR.

Security Incidents

Providers must promptly report all actual or suspected breaches of IT security (including a breach of an External IT System) to both their Departmental Account Management Team and DEWR through their nominated Security Contact, including where any of its Personnel or any Subcontractor suspect that a breach may have occurred or that any entity may be planning to breach IT security. This requirement applies in relation to any actual or suspected IT security breach, regardless of whether the breach is connected to the delivery of the Services or involves access to, or storage of, the Department's information.

Following notification of a breach or suspected breach of IT security, DEWR may review the Provider's incident report and assess the Provider's Accreditation Deliverables to confirm the implementation and effectiveness of relevant security measures. This review is undertaken so that the Department can determine whether the Provider continues to meet the level of assurance required for its assigned Assurance Category.

Based on this assessment, and in addition to any other action the Department may take under the Deed, DEWR may identify corrective actions, require the Provider to undertake an independent audit, or revoke the Provider's RFFR Accreditation where the Provider is assessed as no longer meeting the required level of assurance (see further below). DEWR will notify the Provider of the outcome of its assessment, including whether the Provider's RFFR Accreditation has been revoked and/or any required actions, and the Provider must undertake/implement those actions within the timeframes specified by the Department.

7.5 Other Accreditation events

Revocation

DEWR (in conjunction with the Department) may revoke a Provider's RFFR Accreditation status at any time during the Assurance Lifecycle where the Provider is unable to demonstrate that it continues to meet the security and assurance requirements of its assigned Assurance Category. Without limiting DEWR's discretion, this may include circumstances where the Provider:

- provides false, inaccurate, or materially misleading assurance information,
- fails to provide any additional information to the Department and DEWR within required timeframes,
- does not meet assurance submission or reporting requirements, including where the Provider does not meet those requirements within the required timeframes (without obtaining an extension from the Department),
- does not notify the Department and DEWR of a security incident or breach within required timeframes,
- is subject to a cyber security incident that, as determined by DEWR (in conjunction with the Department), demonstrates fundamental gaps in the Provider's security program, or
- does not notify the Department and DEWR of a change of circumstance impacting its security posture.

Revocation is intended to be an interim assurance measure designed to allow the Provider to restore its security posture. When RFFR Accreditation is revoked:

- the Provider's RFFR Accreditation status will be removed until the required assurance obligations are met,
- DEWR (in conjunction with the Department) will establish a timeframe within which the Provider must regain its RFFR Accreditation status by completing the Reaccreditation stage, and
- the Provider must complete all required assurance activities to successfully complete the Reaccreditation stage within that specified timeframe.

If the Provider does not complete the Reaccreditation stage within the timeframe set by DEWR following the revocation of its RFFR Accreditation status, the Provider may be in breach of its obligations under the Deed.

Re-categorisation

DEWR (in conjunction with the Department) may recategorise a Provider's Assurance Category at any time during the Assurance Lifecycle if the Provider's level of risk exposure to the Department changes. Recategorisation typically occurs when there are significant changes to factors such as:

- the sensitivity or volume of the Department's information handled, and/or
- the nature or scope of Services delivered.

Such changes may increase or decrease the Provider's risk profile and may result in a reassessment of the Provider's Assurance Category.

Following recategorisation of a Provider's Assurance Category by DEWR, DEWR will update the Provider's applicable Assurance Category and will notify the Provider of any revised submission requirements and timeframes for required Deliverables, and/or advise the Provider if it is required to complete the Reaccreditation stage (out of cycle). The Provider must comply with any such requirements within the timeframes advised by DEWR.

Reaccreditation (out of cycle)

If a Provider's RFFR Accreditation is revoked, or the Provider is recategorised to a different Assurance Category, DEWR (in conjunction with the Department) may require the Provider to undergo the Reaccreditation stage outside of the standard three-year cycle.

In such circumstances, the Provider must demonstrate compliance with the assurance requirements of the Provider's Assurance Category. DEWR will notify the Provider of the applicable requirements and the associated timeframes for the out of cycle reaccreditation process. The Provider must comply with any such requirements within the timeframes advised by DEWR.

Extensions

A Provider may request an extension of time where they are unable to meet the timeframes specified in the ESAF or as otherwise required by DEWR, including where additional time is required for:

- the implementation of required security controls,
- the completion of independent audit activities, or

- submitting or updating Deliverables to meet the requirements of the applicable Assurance Lifecycle stage.

A Provider may make a request for an extension of time in writing to SecurityComplianceSupport@dewr.gov.au. The Provider must ensure that any request for an extension of time clearly demonstrates why additional time is required, outlines the Provider's progress in meeting the ESAF requirements to date, and specifies the proposed extension date.

DEWR will forward the request to the Department for decision. The Department will only grant an extension of time in exceptional circumstances and only for the minimum time period necessary.

The Department will consider any request for an extension of time and advise the Provider of the outcome in writing.

ESAF Annual Review

DEWR conducts an annual review of the ESAF and RFFR accreditation requirements to ensure they continue to align with whole-of-government security obligations and DEWR's strategic objectives. This review may result in updates to accreditation requirements, including changes to security control expectations.

Following any review, the Department will notify Providers of any changes to the requirements. Updated templates and supporting documents will be made available on the Department's website.

7.6 Glossary

Term	Definition
Access	Means access or facilitation of access (whether directly or indirectly), traverse, view, use, or interface with, Records or the Department's IT Systems.
Accreditation	The stage of the Assurance Lifecycle where DEWR undertakes a full assessment by the Provider's security posture for RFFR Accreditation, based on the Accreditation Deliverables submitted by the Provider. As part of this assessment, DEWR will evaluate the Provider's service delivery context, data lifecycle, operating model, and implementation of applicable security controls, including any associated risk treatment plans.
Accreditation Deliverables	The documents that a Provider must submit for the Accreditation stage to show that it meets the requirements for RFFR Accreditation for its assigned Assurance Category.
Accreditation Maintenance	The stage of the Assurance Lifecycle during which DEWR conducts annual surveillance reviews focusing on the Provider's progress in implementing outstanding treatment or improvement actions, alignment with any updated RFFR requirements, and any material changes to the Provider's operating model or External IT Systems.
Assurance Category	The category to which a Provider is assigned, based on its overall threat and risk profile, the Services it delivers, and the complexity of its operating environment, in order to determine how much assurance is required for the Provider for the purposes of the ESAF.

Term	Definition
Assurance Lifecycle	The structured set of stages used by DEWR to obtain, maintain, and renew assurance over External IT System/s under the RFFR accreditation approach. It covers all activities, requirements, Deliverables, assessments, timeframes, and obligations for all stages of the RFFR accreditation approach, including the Categorisation, Initial Assessment, Accreditation, Accreditation Maintenance, and Reaccreditation stages.
Categorisation	The stage of the Assurance Lifecycle where DEWR assesses the Provider's service delivery context and operating model to determine the Provider's assigned Assurance Category. The assigned category sets the level of assurance the Provider must provide to achieve and maintain RFFR Accreditation and/or RFFR Reaccreditation.
Categorisation Deliverables	The documents that a Provider must submit for the Categorisation stage to enable DEWR to determine the Provider's Assurance Category.
Deliverables	The documents that a Provider must submit for a particular stage of the Assurance Lifecycle.
Facility	Any physical space in which business is performed to support the provision of the Services, including a building, a floor of a building, or a designated space within a building.
Initial Assessment	The stage of the Assurance Lifecycle where DEWR reviews the Provider's security posture against the requirements of its assigned Assurance Category. Initial Assessment considers how the Services are delivered, the implementation of applicable security controls, and any associated risk treatment plans, and is used to determine whether the Provider is ready to progress to the Accreditation stage.
Initial Assessment Deliverables	The documents that a Provider must submit for the Initial Assessment stage to demonstrate its security posture against the requirements of its Assigned Assurance Category.
Reaccreditation	The stage of the Assurance Lifecycle that occurs: • every three years from the date of the Provider's RFFR Accreditation; and • at other times on an out of cycle basis, where required by DEWR in accordance with the ESAF. This stage of the Assurance Lifecycle involves a full assessment of the Provider's Updated Deliverables by DEWR to confirm that the Provider continues to meet the ESAF requirements for its assigned Assurance Category.
RFFR Accreditation	Accreditation by the Department of the Provider as meeting the requirements of RFFR.
Updated Deliverables	The revised Accreditation Deliverables submitted by a Provider for a particular stage of the Assurance Lifecycle that: • reflect the Provider's current security posture and operating environment; and • are based on the latest applicable DEWR-issued templates, unless transitional arrangements specified in the ESAF apply.