Workforce Australia Guidelines

Part A: Universal Guidelines

Disclaimer

This Guideline is not a stand-alone document and does not contain the entirety of Provider obligations. It must be read in conjunction with the employment services Deed(s) relevant to your organisation (the **Deed**), including any relevant Guidelines and reference material issued by the Department of Employment and Workplace Relations under or in connection with the Deed(s).

This Guideline is 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. This Guideline does not reduce the obligation of Providers to comply with their relevant legal obligations and, to the extent that this Guideline is inconsistent with obligations under the Privacy Act, Social Security Law, the 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 1.17 **Published on:** 4 September 2026 **Effective from:** 1 October 2026

In this version of the Guideline, the Glossary and External Systems Assurance Framework (ESAF) Chapter has been updated.

A full version history of this Guideline can be found on the relevant Archived Guidelines page on the Provider Portal for each program.

Contents

Guideline Interpretation and Glossary		**3**
Chapter 1.	**Operational Requirements**	**6**
Chapter 2.	**Records Management Instructions**	**14**
Chapter 3.	**Privacy**	**24**
Chapter 4.	**External Systems Assurance Framework (ESAF)**	**39**
Chapter 5.	**Servicing Participants with Challenging Behaviours**	**55**

Guideline Interpretation and Glossary

Reading Notes

In this Guideline, ‘must’ means that compliance is mandatory and ‘should’ means that compliance represents best practice for Providers and is expected by the Department.

While reading this document, please note the following Icons and their meaning:



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 work, health and safety.



This icon represents 'Documentary Evidence' – information contained under this dot point will relate to matters of Documentary Evidence.

Glossary

All capitalised terms in this Guideline have the same meaning as in the Deed unless otherwise defined below.

'Accreditation' is the stage of the Assurance Lifecycle where the Department 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, the Department 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' are 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' is the stage of the Assurance Lifecycle during which the Department 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.

'AI Use Case' is a specific application of an AI system or systems by a Provider to achieve certain objectives or perform certain tasks.

'Archives Act' means the *Archives Act 1983* (Cth).

'Assurance Category' is 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.

'Assurance Lifecycle' is the structured set of stages used by the Department 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.

'APP entity' has the same meaning as in section 6 of the Privacy Act.

'Categorisation' is the stage of the Assurance Lifecycle where the Department 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' are the documents that a Provider must submit for the Categorisation stage to enable the Department to determine the Provider's Assurance Category.

'Deed' means any Deed or contract administered by the Department that refers to this Guideline.

'Deliverables' are the documents that a Provider must submit for a particular stage of the RFFR Assurance Lifecycle.

'Employment Services Assessment' or **'ESAt'** means an assessment of a Participant's barriers to employment and work capacity conducted by Services Australia.

'Facility' means 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.

'FOI Act' means the *Freedom of Information Act 1982* (Cth).

'Inactive Records' are Records created under previous contractual arrangements with the Department.

'Incident Report' means a written account of an incident involving challenging behaviour that is recorded on the Department's IT Systems.

'Initial Assessment' is the stage of the RFFR Assurance Lifecycle where the Department 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' are 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.

'Job Capacity Assessment' or **'JCA'** means an assessment conducted by Services Australia to determine eligibility for the Disability Support Pension and includes assessment of barriers to employment and work capacity.

'Job Seeker Snapshot' means a questionnaire completed by a Participant, Services Australia or the Provider, the results of which informs the relevant Participant of the employment services that they are eligible for and supports them in making relevant choices. It includes questions that determine the Participant's Job Seeker Classification Instrument score, support the Participant to make an informed decision where they have a choice between Workforce Australia Online and Workforce Australia Services, and help identify if the Participant requires an Employment Services Assessment.

'Managed Service Plan (MSP)' means an arrangement that a Providers can put in place to tailor the way services are delivered to a Participant who displays challenging behaviours.

'Mutual Obligation Requirement' means any activity test, participation requirement or other requirement that a Participant must meet in order to receive an Income Support Payment.

'One Main Contact (OMC)' means a Participant is restricted to communicating with one identified Provider staff member for the purpose of a Managed Service Plan.

'Protected Information' has the same meaning as in its decapitalised form under section 23 of the *Social Security Act 1991 (Cth)*.

'Reaccreditation' is the stage of the Assurance Lifecycle that occurs:

- every 3 years from the date of the Provider's RFFR Accreditation; and
- at other times on an out of cycle basis, where required by the Department in accordance with the ESAF.

This stage of the Assurance Lifecycle involves a full assessment of the Provider's Updated Deliverables by the Department to confirm that the Provider continues to meet the ESAF requirements for its assigned Assurance Category.

'Referring Provider' means a Provider who Refers an eligible Participant to CTA or EST. For avoidance of doubt, it does not include referrals from Workforce Australia Services or Yarrabah Employment Services to Transition to Work.

'Social Security Law' means the *Social Security Act 1991* (Cth) and *the Social Security (Administration) Act 1999* (Cth), and includes all relevant subordinate legislation and instruments, and the Guide to Social Security Law.

'Unauthorised Access' is the intentional or unintentional action by an entity to make personal information accessible or visible to others outside the entity and which releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.

'Updated Deliverables' are 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 Department-issued templates, unless transitional arrangements specified in the ESAF apply.

Chapter 1. Operational Requirements

Supporting Documents:

- Workforce Australia Brand Style Guide for Providers

1.1. Chapter Overview

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

1.2. Workforce Australia Branding

The Workforce Australia brand has been developed as a masterbrand to frame employment and skills services delivered by the Australian Government. The Department's employment and skills services, programs or initiatives are promoted under this masterbrand.

Providers must use the Workforce Australia masterbrand in the delivery of Services and in accordance with the Workforce Australia Brand Style Guide for Providers (the Brand Style Guide). For the avoidance of any doubt, the Brand Style Guide is a Guideline for the purposes of the employment services Deed(s) relevant to your organisation.

1.3. Recipient Created Tax Invoices

In certain circumstances, including where automatically generated through the Department's IT Systems, the Department may issue a Tax Invoice to the Provider in relation to certain 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 GST Act and will be labelled as an RCTI when issued by the Department. In these circumstances, the Provider is not required to submit a Tax Invoice to the Department, under the Deed.

Where an RCTI is issued by the Department, including where automatically generated through the Department's IT Systems, the Provider acknowledges and agrees that:

- the Department can issue an RCTI to the Provider for the delivery of those Services under the Deed;
- it will not render a Tax Invoice to the Department for the delivery of Services under the Deed for which the RCTI relates; and
- it is registered for GST and it will notify the Department if it ceases to be registered for GST.

The Department acknowledges that it is registered for GST and will notify the Provider if it ceases to be registered for GST.

1.4. Fraud and Corruption Training

To assist Providers in meeting their obligations under the Deed(s) in respect of the prevention of Fraud and Corruption, the Department has developed a Fraud and Corruption training module (available on the Learning Centre). Providers must ensure any of their Personnel who will have access to the Department's IT Systems complete this training.

Providers should be aware of Fraud and Corruption risks that exist within the delivery of employment services and put in place Fraud and Corruption detection practices, policies and procedures, which are

proactively reviewed. Procedures should include a clear reporting process for suspected Fraud or Corruption.

1.4.1. Fraud and Corruption Awareness and Training Expectations

Providers must adopt practices to ensure its Personnel are aware of their obligations under the Deed and this Guideline. Providers must also ensure all Personnel complete the Fraud and Corruption training module:

- upon initial commencement with the Provider; and
- once every 12 months during their engagement.

Providers should note that the Fraud and Corruption training module has been developed to cater for the delivery of all employment services. It is not a substitute for any tailored internal Fraud and Corruption training Providers make available to their Personnel. Providers must consider the nature of the employment services they are delivering and Personnel interaction with those employment services. Where required, the Provider must supplement the Fraud and Corruption training module with its own additional Fraud and Corruption training, within the timeframes above.

1.4.2. Fraud and Corruption Training Module

The Department's Fraud and Corruption training module explains:

- what Fraud and Corruption is
- why people commit Fraud and Corruption, its impact and consequence
- unauthorised access, inadvertent access and conflict of interest
- the legal framework around Fraud and Corruption; and
- how to report Fraud and Corruption.

1.4.3. Personnel Compliance

Providers must monitor and annually self-audit Personnel completion of Fraud and Corruption training. 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 the requirements, where this may be deemed necessary.

Where Fraud and Corruption training is undertaken outside of the Department's Learning Centre, the Provider must retain records of Fraud and Corruption training undertaken by their Personnel and must make this available to the Department on request.

1.4.4. Fraud and Corruption Responsibilities

It is all Personnel's responsibility to report any suspected fraudulent or corrupt activity relating to employment services as soon as they become aware of or suspect it.

When reporting Fraud or Corruption, Personnel should provide as much information as possible, including (where possible):

- **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 which supports the allegation, this information should also be provided.

1.4.5. Reporting Fraud or Corruption

There are a number of mechanisms available to report Fraud and Corruption.

All current and former Personnel of a Provider who suspect Fraud or Corruption should report their concerns to the Department's fraud team via fraud@dewr.gov.au.

Fraud or Corruption can also be reported anonymously via the Department's online reporting tool, Whispli. Whispli allows Personnel to report Fraud or Corruption and communicate directly with the Department without disclosing their identity. Whispli can be accessed via the Department's 'How to Report Fraud and Corruption' webpage.

Conduct by Personnel of a Provider that may breach the Deed or this Guideline, which can include instances of Fraud or Corruption, can be reported to the Employment Services Tip off Line at ESTipOff@dewr.gov.au.

The Public Interest Disclosure Scheme is an avenue for all current and former Personnel of a Provider to report disclosable conduct, which includes suspected Fraud and Corruption, to an authorised officer of the Department, their supervisor, or the Commonwealth Ombudsman. Disclosers will be offered support and protections from reprisal when disclosing under the Public Interest Disclosure Act 2013. Authorised officers can be contacted via PID@dewr.gov.au.

Suspected serious or systemic corruption by or involving current or former Provider Personnel can be reported directly to the National Anti-Corruption Commission (NACC). A range of protections are available to those who report directly to the NACC.

1.5. Dispute Resolution

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

- The Provider will initially discuss the issue or problem directly with a Provider Lead. If the dispute, complaint or problem cannot be resolved, the Provider can request that it be raised with the relevant state manager.
- If the above process does not resolve the issue, the National Contract Manager will attempt to facilitate a resolution.

Any dispute or problem that cannot be resolved through this informal resolution process will be managed through the formal dispute resolution process set out in the relevant Deed.

1.6. Commonwealth Child Safety Framework (CCSF)

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

Where the CCSF is relevant, the Department has included Child Safety clauses into employment services Deeds. As specified in those Deeds, Providers must undertake a range of actions to ensure child-safe

standards and practices are available and implemented. Amongst other things, Providers must comply with applicable Working with Children Laws, obtain Working with Children Checks where required, 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 by completing the Child Safety Provider Declaration within 10 business days of 1 July each year, or if requested by the Department.

1.6.1. Resources for complying with the Child Safety clauses

The Department acknowledges the differences in each organisation, program, and the State and Territory jurisdictions and child safety-related laws. As such, implementation and compliance with the Child Safety clause(s) requires a tailored response from each Provider.

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

1.6.2. Reporting of Incidents

In the course of delivering Services, Providers may identify concerns they have about a Child or Children, whether they are a Participant or not. Providers must ensure that these concerns are actively and appropriately managed in line with their policies and procedures, the National Principles and any legislation in the state and territory jurisdictions they operate in, including those requirements relating to mandatory reporting in those jurisdictions.

Where Providers are complying with the Department's existing processes and policies in the delivery of Services (for example, in incident management or the disclosures of protected information under a Public Interest Certificate), Providers must make the Department aware if a Child or Children are involved and any action taken to manage impact to the Child(ren).

1.7. Minimum Site Requirements

Providers must ensure their Sites meet the following minimum requirements:

- Sites are accessible for people with a disability;
- Sites are presented in a manner that upholds and maintains the good reputation of Services as determined by the Department;
- facilities and protocols are in place to ensure security of personal information and privacy for Participants;
- Sites have a welcoming environment to cater for the needs of Participants and are culturally appropriate;
- for Workforce Australia Services Specialist Providers, Personnel must have experience in delivering services to the specialist participant cohorts that are being serviced at the Site, including access to specialist expertise where required; and
- Sites comply with any relevant State and Commonwealth legislative requirements with regards to health orders or Work Health and Safety.

1.7.1. Co-location with other Providers, Services or Specialist Types

The Department considers a Site to be co-located where more than one Provider, employment service program, (in the case of Workforce Australia Services) specialist type, or third-party organisation is servicing participants at a single Site with any shared space, including reception, waiting areas, servicing areas, and meeting rooms.

In addition to the minimum general requirements for a Site as mentioned above, where multiple Services, specialisations, Providers and/or third-party organisations are co-located at a single Site, the Department requires Providers to at the very least:

- assist Participants or potential service recipients visiting the Site with clear advice about the services delivered at the Site;
- make it clear to individual Participants at the Site what Provider and employment service they have been referred to;
- use clear signage (presented in accordance with the guidance in the Workforce Australia Brand Style Guide section) at reception and the broader workspace aligned with the services being delivered to enable Participants to help them identify where they need to go and who they should talk to upon entry; 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).

1.8. Media Enquiries

Engagement with the media can be an important part of your work as a Provider.

- Providers must immediately refer any media enquiries related to Government policy or program settings to the Department's media team (media@dewr.gov.au), and your Provider Lead and State/Territory Manager. The Department will prepare the response and liaise further with the Minister's media advisers as required. Your email should include the nature and timeframe of the request, as well any relevant background.
- Providers must immediately inform your Provider Lead and State/Territory Manager of any media enquiries received related to your delivery of the Services. Your Provider Lead will then advise whether the media enquiry must be referred to the Department's media team.

1.9. Business Continuity Requirements

The Department defines business continuity as arrangements and practices that ensure there are adequate business processes in place for Providers to continue to meet their service obligations during emergencies or other incidents leading to business disruption.

Providers are required to have appropriate business continuity arrangements in place to ensure the safe provision of employment services to Participants. At a minimum, such arrangements should include processes to:

- contact affected Participants, if required;
- where applicable, ensure that Targeted Compliance Framework (TCF) is not applied where mutual obligation requirements have been suspended;
- arrange alternative servicing options for Participants;
- reschedule activities or appointments, including contacting employers, host organisations, or support services;
- manage site safety and security, including lockdowns or evacuations;

- manage the security and integrity of Provider IT Systems, including containment and notification to the Department of cyber incidents;
- secure records and filing systems; and
- submit urgent/critical notifications and incident reports (including temporary site closure reports) to the Department and other relevant entities (e.g. police, health/welfare agencies, emergency respondents).

1.10. Face-to-face Service Delivery

Face-to-face servicing plays a crucial role in fostering meaningful direct engagement between Providers and Participants in employment services. In-person interactions can allow Providers to gain a better understanding of a Participant's individual circumstances, enabling a more comprehensive tailored experience, resulting in more effective and sustainable employment outcomes.

Within each program's respective Deed and Part B Guidelines, certain Services may be:

- required to be delivered in a face-to-face format (for example, initial interviews, or certain activities), or
- requested by a Participant to be delivered in a face-to-face format where not otherwise required to be delivered face-to-face (for example, ongoing appointments).

This section specifies the conditions that Providers must be satisfied of for Services to be conducted in a face-to-face format. Providers may use this guidance in response to an individual's circumstances, or situations affecting multiple Participants such as natural disasters and health crises (including pandemics).

For clarity, this section does not set out the principles by which Providers should determine whether Contacts or activities that are not required to be face-to-face should be conducted face-to-face. This should be determined through consideration of, and consultation with, Participants and their individual circumstances.

1.10.1. Conditions for the delivery of face-to-face servicing

Providers must consider the Participant's personal circumstances when determining whether Services are able to be delivered in a face-to-face format. In determining this, Providers must be satisfied that face-to-face servicing is:

- **Safe** - Providers must ensure that any face-to-face Service delivery is:
  - carried out in a safe manner
  - appropriate for the relevant Participant, the Provider's staff and others from a work health and safety perspective; and
  - permitted by and consistent with any other legal requirement.

  If a Participant has a history of serious incidents and Managed Service Plans, including at Services Australia, consider if face-to-face servicing is safe or if it will pose risk to other Participants and Provider staff that cannot be reasonably managed at the Site.

- **Beneficial to the individual Participant** - In making this determination, Providers must consider the benefits to a Participant in receiving Services in person, including but not limited to, where a direct and personalised connection with the Provider:
  - is a key element of the service design, for example, in the case of Workforce Australia Services or Transition to Work which requires delivery of high quality, tailored and intensive case management

- where relevant to the program's objectives or Participants' goals, will improve the Participant's prospects for a successful (re)entry into the labour market and ability to find employment
- will help the Participant meet any mutual obligation requirements; or
- will provide the Participant with mental health benefits.

- **Reasonable in the circumstances to be conducted in a face-to-face format** – A list of non-exhaustive circumstances that may make it unreasonable to provide a Participant with Services face-to-face include:
  - they reside in an area that is affected by:
    - extreme weather conditions
    - a natural disaster
    - public transport strikes
    - lack of access to reasonable transport, and/or
    - a written direction as notified by the Department, addressing expectations in relation to Provider servicing arrangements and Participants' Mutual Obligation Requirements.
  - cultural reasons
  - travel time and/or cost is not reasonable
  - they are participating in full-time Education (including training) and this participation restricts their availability to attend face-to-face
  - they are Employed and their hours restrict their availability to attend face-to-face
  - they are subject to legal restrictions (i.e. State or Territory health orders or house arrest)
  - they are not medically fit to attend
  - they have health considerations (including COVID-19 considerations) that impact on the Participant's ability to attend. These may include:
    - being immunocompromised or being a household contact of someone who is immunocompromised, and/or
    - other relevant health considerations.
  - other exceptional circumstances that are beyond the Participant or Provider's control.

  Note: The above reasonable circumstances are also 'Allowable Circumstances' for the purpose of Capability Interviews under the Workforce Australia Services Deed of Standing Offer and relevant Part B Guideline. Providers should be aware of whether there are any directions from the Department relating to the Participants requirements to attend Capability Interviews, for example in relation to extreme weather conditions, natural disasters and public transport strikes.

Alternative Service Delivery

When the conditions for face-to-face servicing are not met or when circumstances beyond the Participant's or Provider's control make it unreasonable to conduct face-to-face servicing, Providers must decide on an appropriate alternative option, which may include:

- rescheduling the appointment
- meeting with the Participant by other means, for example over the phone or online via video conferencing. Please note that Providers are not permitted to meet with Participants at the Participant's home or residence
- placing the Participant in an alternative activity that is not required to be delivered in a face-to-face setting, or
- helping the Participant transfer to a Provider that is more suitable.

For clarity, where face-to-face servicing is a requirement in the respective Deed or Part B Guidelines and exceptional circumstances apply, Providers must make all efforts to reschedule the in-person appointment/meeting/interview/Contact before deciding on an alternative option not involving face-to-face servicing.

Where a Provider determines face-to-face servicing is not appropriate where normally required under the respective Deed or Part B Guidelines, they must record why it is not suitable for the Participant, including what other alternative solutions were explored prior to choosing non-face-to-face delivery.

Unless otherwise provided in the respective Part B Guidelines, Providers must record their reasons in the Comments section of the Department's IT Systems and update their reasons as circumstances change.

For the avoidance of doubt, this is applicable to all Services (including Activities, other courses or training).

Chapter 2. Records Management Instructions

Supporting Documents for this Chapter:

- Employment Services Records Disposal Authority 2003/00330307
- Employment Services Records Authority 2009/0017920
- General Records Authority 31 – Destruction of source or original Records after digitisation, conversion or migration
- General Records Authority 33 – Accredited Training
- Return of Records Process Supporting Document
- Records Register for Provider Returns Spreadsheet
- Records Retention Periods Supporting Document
- General advice on management of Records
- The Office of the Australian Information Commissioner Guide to securing personal information
- Privacy Incident Report

2.1. Chapter Overview

This Chapter outlines Provider obligations with regards to 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 the connection with the delivery of its obligations under and in accordance with the relevant Deed and these 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.

2.2. 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 includes 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:
  - developed or created or required to be developed or created as part of or 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.
- **Provider Records** are all Records, except Commonwealth Records, in existence prior to the relevant Deed Commencement Date:
  - 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, Providers must also take reasonable steps (if any) in the circumstances to ensure that the personal information that the Provider:

- collects is accurate, up-to-date and complete, and
- uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

2.2.1. 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 remain with the Australian Government.

Further information on relevant application and conditions of the GRA 40 is provided on the NAA website.

2.3. 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 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 must be kept securely. The Office of Australian Information Commissioner (OAIC) website provides information on keeping personal identifying information secure.

The Provider must ensure that its:

- Personnel and Subcontractors do not access, copy, disclose or use any:
    - Record containing any information about any participant in any employment services program, 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, and
- Third Party IT Vendors do not access, copy, disclose or use any electronic Record unless such access, copying, disclosure or use is for the purpose of assisting the Provider to comply with the relevant Deed.

Records held by a Provider which were created under a previous Deed (e.g. under the jobactive Deed 2015-2022) must be managed in accordance with the Records management requirements of that previous Deed.

2.3.1. 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 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.

For Records that contain personal information for the purposes of the Privacy Act, in accordance with Australian Privacy Principle 11 as set out in Schedule 1 of the Privacy Act, 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 to protect the Personal Information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure.

Providers must ensure that 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:

- storage environment damage (e.g. for paper Records, damp from a cement floor or fire damage)
- 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, must be kept in lockable cabinets.

2.3.2. Control of Records

Providers must be able to locate and retrieve Records about a Participant if requested. Providers must inform their Provider Lead 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) *(*the *FOI Act)* are able to be located and retrieved efficiently. This includes being able to retrieve email Records and Records created by, or sent to, individuals who have ceased working for Providers.

Records Register

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

The Records register must be created and managed in a digital format (ideally Microsoft Excel or equivalent or a comma or tab limited 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
- Returned – have been returned to the Department.

2.4. Movement of Records

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

- remove any Records relating to the Services, or allow any Records relating to the Services to be removed, from the Provider's premises, except to the extent necessary to enable the delivery of the Services, or
- 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.

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

2.5. Transfer of Records

2.5.1. Transfers 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 Business 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 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.

2.6. Return of Records

Records must be returned to the Department within 28 Business Days if requested by the Department, unless specified otherwise or the retention period has lapsed.

The Records Management Supporting Document has been developed to provide information to Providers on:

- the nature of the return process, including the steps required for the return of both digital and physical Records (where permitted),
- how to determine the Records in scope for any return process and list these in the Records Register for Provider Returns Spreadsheet,
- how to prepare Records to ensure they are successfully returned, including relevant naming conventions, and file organisation, and
- other matters relevant to the returns process.

2.7. Data Migration

Data migration is the process of transferring data from one application or format to another. It may be required when implementing of a new application, which may require data to be moved from an incompatible proprietary data format to a format that is futureproof and can be integrated with new applications.

Providers must ensure that 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 the 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
- 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

This advice is in line with the *Archives Act* and Archives Regulations. However, if future processes include destroying source records, it is recommended that consultation with legal counsel be conducted to ensure that there is no legal requirement to maintain them.

A successful migration demonstrates that the migrated business information is at least functionally equivalent to the source record for business, legal and archival purposes. General Records Authority 31 permits the destruction of information and records after they have been successfully migrated from one system to another.

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.

2.7.1. Data Security Considerations

Providers should be conscious of the following security considerations:

- ensure that those who access sensitive or security classified information have an appropriate security clearance if information is classified, and a need to know that information
- access to (including remote access) to supporting ICT systems, networks, infrastructure and applications is controlled
- information in systems should be continuously safeguarded from cyber threats
- administrative privileges such as logon and administrator privileges should be restricted.

Providers should refer to the digital Information Assurance / IT Security Compliance guide on the Department's website for more information.

2.7.2. Decommissioning of Systems

When decommissioning any systems Providers should ensure that they have considered the value of the business information and any ongoing need to access it. If the information is no longer required, the Provider will need authorisation to legally destroy that information.

The NAA provides authorisation to destroy Australian Government business information in the form of records authorities.

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.

2.8. Breaches and Inappropriate Handling of Records

2.8.1. Reporting Requirements

Providers must report all incidents involving unauthorised access, damaged, destroyed, lost or stolen Records to the Department. Where the Records contain or possibly contain personal information of participants, Providers must follow the Privacy incident reporting process set out in the Privacy Chapter.

2.8.2. 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 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 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.

2.8.3. Notifiable Data Breaches Scheme

All Providers, and the organisations or agencies they share information with, must comply with the requirements of the Notifiable Data Breaches (NDB) scheme in the event of an 'eligible data breach' involving Personal Information.

Information about the NDB scheme and guidance for undertaking an assessment of a privacy incident are available on the OAIC website.

The Department must also be informed of the incident in accordance with the Privacy Incident reporting process set out in the Privacy Chapter and provided with copies of any notifications submitted by the Provider to the OAIC.

2.9. Retention of Records

All Records must be retained by the Provider for a period of no less than 6 years after the creation of the Record, unless otherwise specified in these Records Management Instructions or advised by the Department. For certain Records, specific retention periods are 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). Details of these specific Records and corresponding retention periods are set out in the Records Retention Periods supporting document.

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 source record destroyed.

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

The Department may impose special conditions on a Provider in relation to retention of Records at the Department's absolute discretion. This may include imposing extended record retention periods on Providers.

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 Provider Lead. 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 or as otherwise directed by the Department.

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

2.9.1. Digital Records

Where a Third Party IT Vendor is in possession of Records as a result of assisting a Provider to provide Services under the relevant Deed, the Third Party IT Vendor may only dispose of those Records in accordance with Records Retention Periods with prior agreement of the Provider.

For purposes of determining the applicable retention period, a scanned version of a paper Record would have the same creation date as the original source document.

Information in the Department's IT Systems will be retained by the Department for the appropriate retention periods.

2.9.2. Physical Records

Providers must retain relevant paper Records according to the minimum retention periods outlined in the Deed and, where relevant, the Records Retention Periods supporting document.

2.10. Disposal 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.

2.10.1. 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

- 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.

2.10.2. 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).

2.10.3. General Records Authority 31

Records as defined in the Deed are Commonwealth records for the purposes of the Archives Act.

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.

2.10.4. Destruction of Duplicate Records

Digital Records

Duplicate digital records are to be destroyed in accordance with Methods of Destroying digital Records.

Physical Records

Providers must only destroy duplicate paper records in accordance with NAA guidelines.

Chapter 3. Privacy

Supporting Documents for this Chapter:

- Privacy Notification and Consent Form
- Provider Privacy Incident Report
- Learning Centre: Information Exchange and Privacy Module

3.1. Chapter Overview

This Chapter provides information for Providers and their Personnel on their obligations in relation to handling personal and protected information about individuals, as well in relation to reporting privacy incidents.

3.2. The Australian Privacy Principles

The *Privacy Act 1988* (Cth) (Privacy Act) regulates the collection and handling of personal information through minimum privacy standards, known as the Australian Privacy Principles (APPs).

In delivering Services, Providers collect, use and disclose personal information about individuals. In handling this personal information, Providers are required under their Deed(s) to comply with the Privacy Act and the APPs as if they were agencies. The APPs govern the standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity of personal information
- protection 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.

3.2.1. Personal information and sensitive information

'Personal information' means 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.

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.

When handling personal information, Providers must ensure they are assessing whether the information is also sensitive information, as there are higher standards and additional requirements for collecting, using and disclosing sensitive information. For example, an individual's consent is not required for a Provider (as an APP entity) to collect personal information but will be required for a Provider to collect sensitive information. Inappropriate handling of sensitive information is particularly serious and can result in, amongst other things a requirement to pay compensation or to enter into enforceable undertaking.

3.2.2. Consent and the APPs

In complying with the Privacy Act, the APPs and this Chapter, Providers may be required to seek consent from individuals to permit the handling of their personal and sensitive information. Consent can be given expressly, either orally or in writing, or it can be implied.



In situations of verbal or implied consent, Providers must record the nature of the individual's consent in the Department's IT Systems (where the Provider has access) or in another appropriate format (where the Provider does not have access and which must be made available to the Department on request).

For an individual's consent to be valid, Providers must ensure:

- 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.

Providers must ensure that each individual's consent is regularly reviewed on an ongoing basis (such as in relation to the collection and disclosure of sensitive information under the Privacy Notification and Consent Form, see APP 3: Collection of solicited personal information below).

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.

Further information about consent can be found on the OAIC's website.

3.3. APP 3: 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 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.

3.3.1. Consent to the collection of sensitive information

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

For Providers delivering Services to Participants, during the first meeting with the individual, the Provider must:

- explain the Privacy Notification and Consent Form, and its contents, to the participant, including how their personal and sensitive information will be handled,
- seek the individual's express written consent to collect their sensitive information by asking the individual to sign Part B of the Privacy Notification and Consent Form. Please note Providers may digitise, but must not amend, the Privacy Notification and Consent Form (with the exception of selecting the program from the drop-down menu), and
- advise the individual that they are not required to give consent for the collection of their sensitive information and can withdraw their consent at any time.



Providers must retain copies of the Privacy Notification and Consent Forms signed by individuals in accordance with the Records Management Instructions Chapter and any other Guideline. These must be made available to the Department on request.

While signing the Privacy Notification and Consent Form may indicate express 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 that 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.

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 that they will still be required to participate in the relevant program, however, the lack of consent may limit the options and employment services that a Provider can offer. For example, if an individual does not consent to the collection of sensitive information about their health status or racial or ethnic origin, they may not be referred to any possible appropriate targeted services.



Where an individual withdraws consent to the collection of their sensitive information, the Provider must not destroy the Privacy Notification and Consent Form, except in accordance with the Archives Act, and the Provider must record the withdrawal of the individual's consent to the collection of their sensitive information on the individual's record in the Department's IT Systems (where the Provider has access), or in another appropriate format (where the Provider does not have access and which must be made available to the Department on request).

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

- the collection of the 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 that 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.

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

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

3.4. 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. 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 that it could have collected the personal information under APP 3, or retains the personal information because it is contained in a Commonwealth record, it must handle the information in accordance with the Privacy Act.

3.5. APP 5: Notification of the collection of 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 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.

3.6. 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. 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 Notification and Consent Form.

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 Use and Disclosure of Protected Information).

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.

*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.

3.6.1. Information for 'checks'

Subject to APP 6, Providers must not disclose personal information for the purpose of checks, including police checks, Working with Children Checks, Working with Vulnerable People Checks, Visa Entitlement Verification Online (VEVO) checks and health/medical checks.

If an individual is offered paid work and the Employer seeks one or more of these checks, the Employer should source the information directly from the individual.

When referring an individual to a relevant agency for a check to be undertaken, Providers must ensure that the individual is aware that 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. See deed clauses on 'Checks and reasonable care' for further information.

3.6.2. Tax File Numbers

Providers should also note that the *Privacy (Tax File Number) Rule 2015* (TFN Rule) only allows certain people, agencies, organisations and other entities that are authorised by taxation, personal assistance or superannuation law to ask for and receive TFNs ('authorised or lawful TFN recipients'). A TFN recipient also must not record, collect, use or disclose TFN information unless this is permitted under taxation, personal assistance or superannuation law.

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.

Due to the particular sensitivities attached to TFNs, their use and disclosure are governed by secrecy provisions in applicable legislation. Relevantly, subsection 8WB(1) of the *Taxation Administration Act 1953* (Cth) (TAA) provides that, unless an exception applies, a person must not divulge or communicate another person's TFN to a third person. A breach of subsection 8WB(1) of the TAA may lead to criminal liability.

If TFNs are not authorised to be handled under the TFN Rule or TAA then Providers must redact TFNs from documents before they are stored, used or disclosed.



TFN information must be redacted correctly to ensure the information is permanently removed before uploading documents to the Department's IT Systems. This can be done using one of the following methods:

- Electronic redaction using appropriate software:
    - Use a dedicated redaction tool available through software such Adobe Acrobat, KOFAX Power PDF, or a similar software you may already have.
    - These tools permanently remove the information and sanitise hidden content or metadata.
    - Do not use methods such as placing black boxes, white boxes, or shapes over text, as the underlying information can still be recovered (for example, by deleting or moving the overlay), even after saving as a PDF.
- Manual redaction on hard-copy documents:
    - Redact TFNs using an opaque black marker or similar, ensuring the information is fully obscured and cannot be read or reconstructed.
    - The redacted document must then be scanned to create a new electronic copy before being stored, shared, or processed.
    - The original hard copy must be disposed of in line with records management requirements (See the Records Management Instructions Chapter).

Unauthorised disclosure of a TFN may also amount to a breach of APP 9 including, but not limited to, where a Provider:

- uploads a payslip onto the Department's IT Systems containing a Participant's TFN;
- emails an unintended recipient another Participant's TFN Declaration Form or documentation containing a TFN; or
- uploads a TFN Declaration form onto the Department's IT Systems where the Department has directed such forms be only emailed to the Department.

3.7. APP 7: Direct marketing

APP 7 provides that a Provider must not use or disclose personal information for the purposes of direct marketing unless an exception applies. Prior to undertaking any direct marketing in relation to functions and activities under the Deed(s), Providers must consider whether the proposed marketing is consistent with the Privacy Act. Providers should obtain their own independent legal advice.

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

Providers routinely interact with government related identifiers, including Centrelink Reference Numbers (CRNs), Job Seeker Identification numbers (JSIDs) and TFNs. 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:

- adopt a government related identifier of an individual as its own identifier of the individual, or
- use or disclose a government related identifier of an individual.

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 and should also consider the additional requirements regarding the use and disclosure of Tax File Numbers. Providers should obtain their own independent legal advice.

3.9. 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 that a request to access personal information be made in writing or require an individual to state that 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 directed to the Department for consideration where they encompass records containing information falling within the following categories:

- records also containing information about another person
- medical/psychiatric records (other than those actually supplied by the individual, or where it is clear that the individual has a copy or has previously sighted a copy of the records)
- psychological records, and
- information provided by other third parties.

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 that 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 that they may wish to make a request under the *Freedom of Information Act 1982* (FOI Act). Requests under the FOI Act should be directed to the Department via FOI@dewr.gov.au.

3.9.1. Freedom of Information requests

Under the Deeds, Providers are required to assist the Department in processing requests under the FOI Act 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 or the FOI Act. However, where the document being sought does not contain their personal information, access is not available under the Privacy Act as the Privacy Act only applies to personal information.

Requests under the FOI Act should be directed to the Department via FOI@dewr.gov.au.

3.10. Use and disclosure of Protected Information

Protected Information is information about a person that was obtained by an officer under the Social Security Law and is held or was held in the records of the Department or Services Australia. Protected information may also be personal information under the Privacy Act.

For example, if an individual receives a social security benefit or payment, that individual's information (including their name, date of birth and contact details) will likely be both personal and Protected Information.

Protected information does not include information about a person voluntarily participating in an employment services program. For the purpose of this section, a person is voluntarily participating where they have not applied to receive a social security payment from Services Australia and chooses to participate in an employment program. Information about those individuals will not be protected information, but will still be personal information under the Privacy Act.

3.10.1. Offences related to Protected Information

It is an offence under the *Social Security (Administration) Act 1999* (Administration Act) 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
- otherwise use Protected Information where not permitted.

3.10.2. Permitted uses of Protected Information

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

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

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

3.10.3. 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 information that can be disclosed, the purposes for which the Protected Information can be disclosed and to whom the information can be disclosed. The PIC may also specify who can disclose the information.

Class PICs

The Department's Secretary has issued Social Security (Administration) (Class of Cases) Public Interest Certificate 2022 (the Class PIC). Under the Instrument of Delegation, the Secretary has delegated the power to disclose information in accordance with the Class PIC, to all persons engaged

by an organisation contracted by the Department to deliver employment services for the Commonwealth (i.e. a Provider) who have completed the Department's Information Exchange and Privacy training (available on the Learning Centre). Provider Personnel should be up to date with this training (i.e. completed within the previous 12 months). Each person who meets these criteria is referred to as a 'delegate' for the purposes of the Class PIC.

Under the Social Security Law and as relevant to the delivery of employment services by Providers, an 'officer' for the purposes of the Class PIC and Instrument of Delegation includes:

- a person performing duties, or exercising powers or functions, under or in relation to the Social Security Law, or
- a person who, although not appointed or employed by the Commonwealth, performs or did perform services for the Commonwealth and who, as a result of performing those services, may acquire or has acquired information concerning a person under the social security law

As such, an 'officer' can include Personnel who are both directly and indirectly involved in the delivery of services to a Participant or other person under the Social Security Law. For example, Personnel in administration or governance roles, or Personnel delivering non-vocational assistance (such as allied health professionals), may be 'officers' for the purposes of the Class PIC and Instrument of Delegation.



Provider Personnel who need to complete the Department's Information Exchange and Privacy training on the Learning Centre to be a Class PIC delegate, but do not require access to other parts of the Department's IT Systems such as Workforce Australia Online, must be set up in Employment Security Access Management (eSAM) using:

- the base role of 'NIL', and
- the relevant contract type (e.g. PRO6, CTA6, EST6 etc.).

This may be relevant for roles such as training facilitators or allied health professionals employed by a Provider and will enable access to the Learning Centre to complete the Information Exchange and Privacy training, without granting wider access to Participant information.

Preventing or lessening a threat

A delegate may disclose Protected Information about an individual under the Class PIC to police, emergency services, an emergency call service "Triple Zero", health service providers, or child protection agencies:

- where the person making the request cannot reasonably obtain the information from another source, and
- the individual to whom the information relates is unable, refuses, or is likely to refuse to provide information to those specific persons, and
- disclosure of the information is necessary to prevent or lessen a threat to the life, health or welfare of a person.

Offences against the Commonwealth, Commonwealth officers, or offences in Provider premises

A delegate may also disclose Protected Information about an individual to the police under the Class PIC:

- where the police cannot reasonably obtain the information from another source, and

- the individual to whom the information relates is unable, refuses, or is likely to refuse to provide information to the police, and
- the disclosure of the information is necessary because an offence or threatened offence has occurred against an officer, or against Commonwealth property, or in premises occupied by an organisation contracted by the Department to provide employment services for the Commonwealth.

Process for disclosure under the Class PIC

The delegate must consider the facts of the case and determine if the Class PIC applies. A delegate may consult with others (to the extent Social Security Law allows) to determine if the Class PIC applies and, if so, who may be best placed to disclose the information.

Where a delegate has determined that the Class PIC applies to a situation, the delegate should only disclose the Protected Information about an individual that is relevant to the purpose. The Protected Information that may be disclosed where relevant is:

- the full name, any previous names and any other names the person is known by
- any contact details (including postal or residential addresses) and telephone numbers; and
- any other information necessary to the purpose for which the information is needed. For example, it is unlikely that providing a Participant's JSID or Tax File Number will be necessary for any of the purposes specified in the Class PIC. Delegates must ensure that disclosures of information under the Class PIC do not incidentally or otherwise release unnecessary information, including the information of unrelated individuals.

Once the delegate has disclosed the information, they must complete the Release of Protected Information Notification Form. Once completed, the Provider must send the completed form to their Provider Lead as soon as possible and within 48 hours of the disclosure of information.

Process for disclosure of CCTV footage

Providers may be asked by police or other third party requestors for copies of CCTV footage to assist in the investigation of the types of offences referred to in the Class PIC. Where the CCTV footage contains personal information or Protected Information of multiple individuals, Provider staff should not disclose the CCTV footage to police or third party requestors under the Class PIC. If a Provider receives a request for CCTV footage containing Protected Information, or otherwise wishes to disclose such footage to a third party, the request should be sent to their Provider Lead for consideration by the Department of whether a Specific PIC can be issued. See Specific PICs below for information on what to include in this request. CCTV footage obtained broadly for security and safety purposes, and not associated with the servicing of Participants, is unlikely to be Protected Information.

Specific PICs

Providers are required to obtain a specific PIC to release Protected Information in situations that are not covered by the Class PIC and disclosure is not otherwise authorised, such as lack of consent of the individual or individuals. Examples include:

- releasing Protected Information to Police or other authorities where the Class PIC does not apply, such as when there is no threat to anyone's life, health or welfare; and
- responding to a subpoena or other notice requiring production of documents.

Providers will need to approach the Department through their Provider Lead (in writing) to request consideration of issuing a specific PIC. Providers should make the request as soon as they become aware of circumstances where they wish to, or are being asked to, disclose Protected Information to ensure the Department has sufficient time to review and respond to the request.

As part of any request to the Department, Providers must provide a copy of any request from a third party they have received, and as many details as possible about why the specific PIC is being sought, including the following:

- who the request was made by, their contact person and phone number
- why the information is required by the person making the request
- why the information could not be obtained from another source (e.g. what other steps they have taken to try to obtain the information and the outcome of those steps)
- if the request relates to a breach or an alleged breach of a law (criminal or otherwise):
    - what the breach or alleged breach is, including the legislation involved
    - the details of imprisonment and/or pecuniary penalties; and
    - the details surrounding the breach.
- if the request may require the disclosure of CCTV footage:
    - a summary of what the footage shows, including the relevant individuals visible in the footage and whether they are Participants, Personnel or other third parties (such as bystanders or witnesses)
    - a copy of the footage, where reasonably available to be extracted and provided to the Department
    - reason for the existence of the CCTV footage; and
    - confirmation as to whether the Provider is holding footage in the records of the Department, or whether footage is taken on the Department's behalf (and if this footage is made available to the Department).
- the information that is to be released
- the due date of the request, if applicable. For example, a deadline specified by a subpoena; and
- the Provider's assessment of the request, including its assessment of the appropriateness under the Class PIC and why it may not be appropriate to seek the relevant Participant's consent to the disclosure.

The Department will not issue a specific PIC in every case and the Provider should obtain their own independent legal advice before responding to the request for, or otherwise disclosing, Protected Information. Please note, the Department will endeavour to respond to each request before any specified due date or deadline that is reasonable, however, this may not always be possible, and Providers should ensure that they obtain their own independent legal advice.

Subpoenas or notices to produce

If a Provider receives a subpoena or a notice to produce from a court which requires disclosure of Protected Information, the Provider must ensure that they comply with all relevant laws, as well as the requirements of the Deed and Guidelines, in responding to that subpoena or notice to produce.

In particular, Providers should have regard to section 207 of the Administration Act in determining whether a Participant's Protected Information can be disclosed. Providers should obtain their own legal advice, where relevant.

Providers do not need to contact the Department if the Participant has consented to the release of the information to a nominated recipient for a specified purpose as requested under a subpoena or notice to produce, irrespective of whether it is related to employment services. For example, if a Participant is in an unrelated motor vehicle incident, they might claim compensation and the relevant insurer might want access to Protected Information about a Participant held by the Provider to help assess the Participant's claim. The Department takes the position that the Protected Information could be disclosed to the court if the Participant consents and that it would be acceptable for the Provider to seek the Participant's consent if the insurer has not already supplied the Provider with evidence of their consent.

3.11. 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
- this is likely to result in serious harm to any of the individuals to whom the information relates, and
- the entity has been unable to prevent the likely risk of serious harm with remedial action.

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 that 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 that their privacy has been interfered with.

Providers should be aware that 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.

3.12. Privacy complaints

An individual who considers that 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 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.

3.13. 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.

Individuals may contact the Department via privacy@dewr.gov.au.

For further information and alternative contact details, please refer to the Department of Employment and Workplace Relations' Privacy Policy.

3.14. Awareness and Training Expectations

Providers must adopt practices to ensure its Personnel are aware of their obligations under the Privacy Act, the Deed and this Chapter. Providers who have access to the Department's IT Systems must ensure that all 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 module (training module), available on the Learning Centre:

- prior to delivering the Services; and
- at least once every 12 months.

Provider Personnel who need to complete the Department's Information Exchange and Privacy training on the Learning Centre in accordance with this section, but do not require access to other parts of the Department's IT Systems such as Workforce Australia Online, must be set up in Employment Security Access Management (eSAM) using:

- the base role of 'NIL', and
- the relevant contract type (e.g. PRO6, CTA6, EST6 etc.).

This may be relevant for roles such as training facilitators or allied health professionals employed by a Provider and will enable access to the Learning Centre to complete the Information Exchange and Privacy training, without granting wider access to Participant information.

Providers should note that the Department's privacy training module has been developed to cater for the delivery of all employment services. It is not a substitute for any tailored internal privacy training Providers make available to their Personnel. Providers must consider the nature of the employment services they are delivering and Personnel interaction with personal information for those employment services. Where required, the Provider must supplement the Department's privacy training module with its own additional privacy training, within the timeframes above.

3.14.1. Information Exchange and Privacy Module

The Department's Information Exchange and Privacy module explains the key concepts under the Privacy Act 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 all Personnel handling personal information 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, taking into account compliance with new laws or updated information handling practices, and ensuring that they are responsive to new privacy risks.

3.14.2. Personnel Compliance

Providers must monitor and annually self-audit Personnel 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 Personnel and must make this available to the Department on request.

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

Chapter 4. External Systems Assurance Framework (ESAF)

4.1. Chapter Overview

This Chapter sets out the External Systems Assurance Framework (ESAF) 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 relevant Deed, and the Department may take action against the Provider in relation to the breach in accordance with the Deed.

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 relevant Deed.

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

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

4.2. Templates and other resources

Providers must ensure that all information provided to the Department 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, the Department 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.

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

4.3. RFFR Core Expectations

Under the ESAF, each Provider is assigned to one of 4 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.

4.3.1. 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.

4.3.2. 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.

4.3.3. Cyber Security

Providers must establish, implement, and maintain cyber security measures proportionate to their risk profile, to minimise the risk of Department 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 relevant 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 ICT 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.

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

Where under the relevant 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.

4.3.5. 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 the Department 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 the Department in relation to the TPES System,
- confirm that the TPES System is currently included in the list of accredited TPES Systems published on the Department'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'.

The Department's accreditation of a TPES System provides assurance that the TPES System meets the Department'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. The Department 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 the Department 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.

4.4. Right fit For Risk (RFFR)

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

4.4.1. Assurance Lifecycle

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

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

Table 4-A: Assurance Lifecycle

Assurance Lifecycle stage	Timeline
Categorisation	The Provider must complete the Categorisation stage within **one month** of the Deed Commencement Date of the relevant Deed.
Initial Assessment	The Provider must submit the Initial Assessment Deliverables within **two months** of the Deed Commencement Date of the relevant Deed. The Provider must complete the Initial Assessment stage within **3 months** of the relevant Deed Commencement Date.
Accreditation	The Provider must submit the Accreditation Deliverables at least **6 weeks** before the Provider is required to obtain RFFR Accreditation. The Provider must obtain RFFR Accreditation within **9 months** of the relevant Deed Commencement Date.
Accreditation Maintenance	The Provider must submit Updated Deliverables at least **6 weeks** before the Provider is required to complete the Accreditation Maintenance stage.

Assurance Lifecycle stage	Timeline
	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 **6 weeks** before the Provider is required to complete the Reaccreditation stage. The Provider must complete the Reaccreditation stage every **3 years** from the date that RFFR Accreditation was obtained.

4.4.2. Categorisation

Categorisation is the first stage of the Assurance Lifecycle and is used by the Department to determine the Provider's Assurance Category. The Assurance Category that is assigned by the Department 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 4-B, within **one month** of the relevant Deed Commencement Date.

Table 4-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 Request for Proposal or Request for Tender.
Categorisation Meeting	The Provider must attend a Categorisation Meeting with the Department for the purposes of: • validating the information provided by the Provider in the Categorisation Questionnaire, • enabling the Department 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	The Department 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 the Department 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 the Department 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 the Department'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, the Department will assign to the Provider the Assurance Category that best reflects the Provider's overall threat and risk profile. The 4 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.

4.4.3. Initial Assessment

The Initial Assessment stage involves an assessment by the Department 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 the Department 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 4-C below, within **two months** of the relevant Deed Commencement Date. This timeframe is to allow the Department to complete the Initial Assessment stage within **3 months** of the Deed Commencement Date.

Where the Department determines that the submitted Initial Assessment Deliverables do not clearly demonstrate the Provider's security posture, the Department 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 the Department determines that additional time is required for the Provider to address identified deficiencies.

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

Table 4-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 Department 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 2	• 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 Department 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	• 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 Department 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 the Department'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 the Department:

- a completed System Security Plan (SSP) clearly defining the scope of the TPES System and security controls in place to safeguard Department 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.

4.4.4. Accreditation Stage

The Provider must achieve RFFR Accreditation within 9 months **of the relevant Deed Commencement Date. The Provider must submit all required Accreditation Deliverables, as specified in**
Table 4-D below, no later **than 6 weeks** prior to the deadline for achieving RFFR Accreditation.

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

The Department will assess the Provider's security posture for RFFR Accreditation based on the Accreditation Deliverables submitted by the Provider, as specified in
Table 4-D. As part of this assessment, the Department 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 the Department determines that the submitted Accreditation Deliverables do not clearly demonstrate the Provider's security posture, the Department 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 the Department 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 the Department, following the Department'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 **3 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 4-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 Department information.
Category 2	• 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 Department information.
Category 1	• 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 Department 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 the Department'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 the Department:

- 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 Department 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.

4.4.5. 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 Department 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 **6 weeks** before each Accreditation Maintenance Date, the Provider must submit to the Department the Updated Deliverables. The Updated Deliverables must reflect the Provider's current operating environment and External IT Systems.

Where the Department determines that the Updated Deliverables do not clearly demonstrate the Provider's security posture, the Department 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 the Department determines additional time is required for the Provider to address identified deficiencies.

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

4.4.6. Reaccreditation stage

The Reaccreditation stage involves a full reassessment by the Department 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 **6 weeks** before the Reaccreditation Date, the Provider must submit to the Department the Updated Deliverables. The Updated Deliverables must reflect the Provider's current operating environment and External IT Systems.

Where the Department determines that the submitted Updated Deliverables do not clearly demonstrate the Provider's security posture, the Department 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 the Department 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. The Department will notify the Provider once it has successfully completed the Reaccreditation stage.

4.5. Reporting Requirements

4.5.1. Change of Circumstances

The Provider must notify the Department 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. 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.

The Department 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 the Department any additional information within the timeframes requested by the Department.

4.5.2. Security Incidents

Providers must promptly report all actual or suspected breaches of IT security (including a breach of an External IT System) to the Department 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, Department information.

Following notification of a breach or suspected breach of IT security, the Department 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, the Department 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). The Department 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.

4.6. Other Accreditation events

4.6.1. Accreditation Revocation

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 the Department'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 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 of a security incident or breach within required timeframes,
- is subject to a cyber security incident that, as determined by the Department, demonstrates fundamental gaps in the Provider's security program, or
- does not notify the Department 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,
- 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 the Department following the revocation of its RFFR Accreditation status, the Provider may be in breach of its obligations under the relevant Deed.

4.6.2. Recategorisation

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 Department 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 the Department, the Department 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 the Department.

4.6.3. Reaccreditation (out of cycle)

If a Provider's RFFR Accreditation is revoked, or the Provider is recategorised to a different Assurance Category, 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. The Department 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 the Department.

4.6.4. 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 the Department, 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.

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.

4.7. ESAF Annual Review

The Department conducts an annual review of the ESAF and RFFR accreditation requirements to ensure they continue to align with whole-of-government security obligations and the Department'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.

4.8. Use of Artificial Intelligence in Service Delivery

This section sets out Providers' obligations relating to the use of Artificial Intelligence (AI) in the delivery of Services.

The requirements in this section are intended to maintain the integrity, security, and ethical standards in the delivery of Services, and to ensure that Providers' use of AI is consistent with the Digital Transformation Agency's Policy for the responsible use of AI in government and the Department's privacy and information security requirements.

Providers' compliance with this section will help maintain public trust and ensure the effective and responsible delivery of Services.

In this section, **'AI Technologies'** means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. AI Technologies may vary in their levels of autonomy and adaptiveness after deployment. This may include AI technologies such as machine learning, natural language processing, and generative AI tools.

4.8.1. Providers' requirements relating to the use of Artificial Intelligence

The Department is committed to realising the benefits of AI by engaging with AI confidently, safely, and responsibly. As such, the Department will permit the use of AI by Providers in the delivery of Services but **only where** the Department gives its explicit approval to the specific AI Use Case for the delivery of Services **and** provided that the following conditions are met:

1. The AI Use Case does not involve AI Technologies banned by the Australian Government.
    - The Australian Government or the Department may from time-to-time advise or notify Providers of AI Technologies that are banned. Australian Government advice is provided in the Protective Security Policy Framework Publication Library.
    - The Department advises the following as banned AI Technologies:
        - products and web services from DeepSeek and Kaspersky Lab, Inc. This is consistent with the Department of Home Affairs' guidance to Commonwealth Agencies (see Direction 001-2025 and Direction 002-2025).

- Providers must ensure the AI Use Case upholds ethical principles, privacy and data protection laws, and contractual requirements with respect to information management (including in relation to intellectual property, confidentiality and Records management).

- This includes ensuring that the AI Use Case:
  - safeguards personal, sensitive and protected information,
  - does not compromise the privacy of individuals,
  - does not involve automated decision-making, and
  - ensures the keeping of detailed records.
- The AI Use Case must not include the use of AI bots for the purposes of recording meetings with the Department.
- Providers wishing to use AI bots to record meetings with Participants must seek prior written approval from the Department in accordance with the Third-Party AI Assessment Framework.
- Providers are responsible for managing compliance with these principles, relevant laws and contractual requirements in implementing and maintaining the AI Use Case, and for otherwise meeting their contractual obligations.

2. Providers must ensure that any AI Use Case implemented within their External IT Systems adheres to the cyber security requirements outlined in the Australian Government Information Security Manual (ISM) and the Protective Security Policy Framework (PSPF) to ensure the secure operation of all systems.

A Provider who would like to request to use AI in delivering Services should refer to the Third-Party AI Assessment Framework and Application Form. The Provider must make any request for approval of an AI Use Case by sending the completed application form to SecurityComplianceSupport@dewr.gov.au, copying in their Provider Lead(s). Any request must address in detail that the conditions above have been satisfied by the Provider.

Providers may utilise AI Technologies for functions not directly related to the delivery of Services without approval from the Department. Providers are responsible for ensuring any AI Use Case being used for such purposes is isolated from all aspects of the delivery of Services. If isolation cannot be ensured, the AI must not be used unless approved by the Department.

Chapter 5. Servicing Participants with Challenging Behaviours

5.1. Chapter Overview

This Chapter provides information for Providers on recognising and managing challenging behaviour. It includes information on how to continue servicing Participants with challenging behaviours so that they can remain connected with Services and (where applicable) meet their Mutual Obligation Requirements, while limiting risks to the safety of Provider staff, Participants and property.

All Providers are responsible for ensuring people's safety on their premises and that the Services they deliver are carried out safely. Providers should adapt the strategies that are outlined in this Chapter to suit their own circumstances. This Chapter supplements, and does not replace, Provider internal operational policies and procedures. Providers are responsible for informing themselves of their relevant legal and Deed obligations, including relevant Work Health and Safety (WHS) and Privacy Laws, and ensuring compliance with these obligations. This Chapter does not cover WHS incidents. WHS incidents must be reported in accordance with Deed requirements.

This Chapter provides guidance on Recognising challenging behaviour and on Managing a challenging behaviour incident.

The Incident reporting and post-incident servicing sections provide guidance on servicing strategies for Participants with challenging behaviour. This includes incident notification requirements, Incident Reporting and Managed Service Plans (MSPs) for Participants with challenging behaviours.

5.2. Recognising challenging behaviour

Challenging behaviour is any behaviour that a reasonable person would consider unacceptable or hostile and that creates an intimidating, frightening, threatening, offensive or physically dangerous situation in the workplace or other location.

Challenging behaviours may include but are not limited to:

- physical violence against any person—for example, hitting, kicking, punching, spitting on or throwing objects at a person
- acting in a way that would cause a person to have a reasonable belief that assault was intended
- adopting a physical position or state and/or producing an object that a reasonable person would consider constitutes a serious and/or imminent threat of physical violence
- oral or written (for example, email or communication through social media) threats, abuse or harassment, inappropriate touching or stalking of staff members or other Participants
- damaging, defacing or destroying property intentionally or through inappropriate and aggressive behaviour such as throwing objects or punching and kicking property
- theft of property, illicit drug taking on the Provider's premises, use of the Provider's equipment and/or property for illegal purposes
- swearing, making offensive noises or gestures, inappropriate or suggestive comments, vilification

- causing injury to oneself—for example, cutting or indications of suicide or self-harm
- any other behaviour that is deemed inappropriate and warrants an incident being recorded.

A Participant may demonstrate challenging behaviour through digital interactions (including over the phone, email and/or social media), written communication and/or face-to-face interactions (for example at the Provider's office or while attending training, courses, work placements or internships).

5.3. Managing a challenging behaviour incident

The Department views the safety of Provider staff and Participants as a priority and acknowledges that Providers have a wide variety of expertise and arrangements in place to address safety concerns and challenging behaviours.

Providers are responsible for ensuring people's safety on their premises and that the Services they deliver are carried out safely. Where challenging behaviour is observed, Providers should consider whether police involvement is required and are encouraged to contact police if they believe assistance from emergency services is necessary.

5.3.1. Maintaining an incident management plan

It is the Provider's responsibility to have an incident management plan in place that outlines its approach to managing situations where Participants, staff or visitors display challenging behaviours, or where Provider staff identify that a situation has the potential to escalate to become an incident.

5.3.2. General considerations

Strategies may differ between Providers and their sites. Participants' circumstances differ and there may be a range of factors that contribute to incidents of challenging behaviour and the most appropriate strategy for the management of that behaviour.

When Providers are dealing with a case of challenging behaviour, they may wish to discuss the Participant's behaviour with them. Participants have the right to ask questions and appropriately outline their views on their entitlements and servicing. As long as they are not being abusive or using offensive language, Participants should not be considered as demonstrating challenging behaviours in these situations.

Participants bringing children to appointments or activities, including under the ParentsNext program, are responsible for the behaviour of their children. Providers must take reasonable steps to ensure the safety of Provider staff, other Participants and the general public in the delivery of Services at their premises, even from children exhibiting challenging behaviours. Providers may require that a Participant remove their child from the premises where the child's behaviour poses a threat to others and should contact emergency services if necessary.

Where a Participant demonstrates challenging behaviour while participating in an activity, the Provider should take any appropriate action in accordance with the situation and their Deed and WHS Laws. For example, refer to the Temporary Site Closure document on the Provider Portal or the information provided below. Also, see Incident Reporting and Post-Incident Servicing.

Providers should also discuss with the Referring Provider, or the Digital Services Contact Centre (the DSCC) in the case of Workforce Australia Online Participants (or via the Provider Lead where necessary), prior to exiting the Participant from a course.

5.3.3. Information sharing between Providers and Services Australia

It is important that Providers make connections with their local Services Australia offices and build effective working relationships to facilitate information sharing, including incident notifications, having regard to the Privacy Chapter. Providers should contact their Provider Lead if support is required to engage with Services Australia.

5.3.4. Immediate notification requirement

Where an incident has occurred and the Provider has reason to believe that the Participant who is displaying threatening, aggressive or violent behaviour poses a serious threat to the life, health or safety of an individual, the Provider should immediately call 000 and advise them of the situation, then follow the Public Interest Certificate (PIC)/Class PIC requirements (see Use and disclosure of Protected Information).

Notifying Services Australia

Given the shared interaction of Participants with Workforce Australia and Services Australia, where a Participant has made threats towards Services Australia staff, it is essential that information on these threats is escalated to keep staff and other Services Australia customers safe.

- In the first instance, the Provider should attempt to call the Services Australia Service Centre (the office closest to the Provider's location or the location of a threat) to advise of the risk.
- If the Provider is unable to contact the local Services Australia Office or is not sure who to call, they should:
    - phone the Services Australia Security Hotline on 1800 046 021
    - this hotline is managed by Services Australia Regional Security Advisers and is operational nationally between 7.00 am and 7.00 pm Monday to Friday
    - the Regional Security Advisers will ensure that the issue is escalated appropriately.

In the event of an emergency - call 000.

5.3.5. Temporary Site closures

Where Providers experience incidents involving Participants with violent, aggressive or threatening behaviours, they may elect to temporarily close the affected Site until the situation is resolved or until they are satisfied the threat no longer exists. Please refer to the Temporary Site Closure requirements on the Provider Portal.

5.3.6. Disclosing personal and sensitive information

Providers are responsible for ensuring they are aware of and comply with their legal obligations for the handling, use and disclosure of personal and sensitive information.

For information on disclosing personal information and Protected Information refer to the APP 6: Use and Disclosure of Personal Information section of the Privacy Chapter.

For information on disclosure of Protected Information under the Social Security Administration - Class of Cases - Public Interest Certificate (No. 1) 2022 (Class PIC), including who can disclose information under the Class PIC and when information can be disclosed under the Class PIC refer to the Public Interest Certificates section of the Privacy Chapter.

5.4. Incident reporting

The challenging behaviour incident reporting arrangements detailed in this section have been established for Providers delivering the following programs:

- Workforce Australia Services
- Workforce Australia - Transition to Work Services
- Workforce Australia - Career Transition Assistance
- Workforce Australia - Employability Skills Training
- Harvest Trail Services
- Self-Employment Assistance
- ParentsNext
- Workforce Specialists
- Norfolk Island
- Yarrabah Employment Services
- Broome Employment Services

5.4.1. Incident reporting

Providers are required to submit an Incident Report after each Challenging Behaviour Incident, including a completed Incident Details section for each Incident Report. Guidance to assist with these steps is provided in the tables and system steps below.

The purpose of the Incident reporting arrangements is to have a written record of incidents involving challenging behaviour to inform Provider and Services Australia frontline staff of the potential for further incidents, support compliance measures where appropriate and assist Providers to manage the safety of their staff.

The arrangements are designed to make Participants' experiences more consistent across both the Department and Services Australia by aligning processes and terminology for managing challenging behaviour with those used by Services Australia. This is achieved through the use of:

- an **Incident Severity Matrix** – an automated process which assigns a severity level to an incident. The matrix removes subjectivity when determining the severity of an incident based on key information about the incident. The matrix assesses the importance of all incidents being considered in the context of 'organisational tolerance' not 'personal tolerance'; and
- **Managed Service Plans (MSPs)** – arrangements that Providers can put in place to tailor the way Services are delivered to Participants who display challenging behaviours.



Providers must complete an Incident Report for all incidents where a Participant exhibits challenging behaviour, including where it has resulted in a Temporary Site closure, in the Incident Report screen in the Department's IT Systems (see the Completing an Incident Report section).

5.4.2. Completing an Incident Report

Completing an Incident Report ensures all staff are informed about the history of a Participant's challenging behaviour so they can make an assessment on the likelihood of further incidents and determine appropriate future servicing arrangements to minimise risks to people and property.

Accurate recording of incidents ensures that, if the Participant is transferred to another Site or Provider, the receiving Site or Provider is aware of the challenging behaviour/s and can arrange to service the Participant accordingly.

A challenging behaviour incident may also be considered a WHS incident. In these cases, the Provider may need to submit an Incident Report and also Notify the Department of the WHS incident in accordance with Deed requirements.

When creating an Incident Report, Providers should consider that under the FOI Act, a person has the right (with limited exceptions) to access their personal information or documents held by the Department or Providers.

Providers should ensure that, when creating an Incident Report, all records are factual, comprehensive, free from jargon and do not include unnecessary or inappropriate commentary. When considering whether information is necessary, an incident report must convey the severity and specific details of any threat so using the exact wording used in the incident, including strong language and words expressing violent actions, may well be appropriate.

Records created by the Department or Providers may also be released as part of Court proceedings.

The tables below outline descriptions for the terms used for reporting incidents in the Department's IT Systems - please select all categories that apply. Please note, only the 'comment' and 'police reference number' fields can be edited after submitting an Incident Report.

Table 5-A: Challenging Behaviour Incident Reporting Terminology - Types of Incidents

Type	Behaviour or action displayed during the incident
Assault – no weapon	Actual, attempted or threat of physical attack: • strike • touch or • applies force • spitting • without a weapon, either directly or indirectly upon a person.
Assault – weapon	Actual, attempted or threat of physical attack • strike • touch or • applies force • with a weapon (including an improvised weapon), either directly or indirectly upon a person.

Type	Behaviour or action displayed during the incident
Health and Safety	Any event where the person requires first aid or medical attention due to: • physical or psychological injury • stress reaction • illness • disease • or exposure.
Self-Harm	Any incident where a person causes or indicates deliberate injury to themselves
Abuse	The use of language: • to insult or cause offence • such as discriminatory language based on the grounds of age, disability, race, religion, sex, intersex status, gender identity and sexual orientation.
Behaviour	Any incident where a customer acts in a counterproductive manner, including: • offensive language • gestures • refusal to leave or disruptive on premises • excessive contacts • intimidation/coercion • harassment and stalking.
Property	Any incident where a person causes damage to the property and/or damage to contents of the property i.e. furniture or office equipment within the Site

Table 5-B: Challenging Behaviour Incident Reporting Terminology - Nature of Incident

Nature of Incident	Description
Actual	Where there is a factual occurrence
Threat – Provider	Expression of the intention to do something to the Provider
Threat - Other	Expression of the intention to do something to an 'other' person/organisation

Table 5-C: Challenging Behaviour Incident Reporting Terminology - Emergency Services and Site Safety Impact

Action	Impact

Were the emergency services contacted?	The Incident required assistance from 000 emergency services (either during or after the Incident) If yes, how many of the emergency services were contacted (select multiple options if relevant)? • Police • Ambulance • Fire
What is the number for Police reference recorded?	Police event number
Was the site safety impacted?	If yes, how was site safety impacted (select multiple options if relevant)? • Impacted Provider staff (with injury) • Impacted Provider other (with injury) • Non-compliance with restriction • Site closure Refer to Table 5-D for further information.

Table 5-D: Challenging Behaviour Incident Reporting Terminology - Site Impact

Impact	Description
Impact Provider staff (with injury)	Where the Provider staff was physically or psychologically injured
Impact Provider other (with injury)	Where an 'other' person/organisation was physically or psychologically injured (note: this could include another Participant, a Security Guard, a member of public or family member of a Participant).
Non-compliance with restriction	Breach of existing service channel restrictions applied under an MSP and the Participant displays aggressive or counter-productive behaviour and a refusal to leave when reminded of the MSP. Note: Selecting this category as an Impact will increase the severity level of the Incident. If the Participant leaves immediately when reminded of the MSP and does not display challenging behaviours during the interaction - an incident record is not required.
Site Closure	Where the incident warranted a Temporary Site Closure

Providers must record an Incident Report in the incident report screen in the Department's IT Systems where a Participant exhibits challenging behaviour. Incidents should be recorded on the day the incident occurred or as soon as possible and within 24 hours.

Where it is not possible for the staff member who witnessed the incident to complete the Incident Report, another staff member should do so on their behalf.

The Department's IT Systems allows an Incident Report to be backdated up to 14 calendar days. If Providers are unable to record an incident in the Department's IT Systems due to technical issues, Providers must notify the Department as soon as possible and create an Incident Report in the Department's IT Systems at the earliest opportunity.

When recording an Incident Report, you can select multiple options in the following sections:

- What is the nature of the incident? e.g. Actual + Threat Provider + Threat – Other
- What type of incident occurred? e.g. Assault – Weapon + Abuse + Behaviour + Property

'Incident Detail' – It is mandatory for Provider staff to include incident details in the Incident Report. This will assist Provider and Services Australia staff to manage the safety and wellbeing of staff, other Participants and the general public. It will also assist with post-incident servicing of the Participant.

Ensure all records are factual, comprehensive, free from jargon and do not include unnecessary or inappropriate commentary. It is important to include the words and language the participant has displayed at the time of the incident. This will ensure that any future behavioural concerns are clearly identified and support assessment of whether the Participant's behaviour is escalating.

Table 5-E: Challenging Behaviour Incident Reporting Terminology – Examples of Incidents

Example of incident	Nature of the incident	Type of incident	Emergency Services	Site safety impacted
'Participant 1 attended the site today and started yelling. He demanded that we restore his payments. I explained he needs to visit Centrelink to discuss. Participant 1 swore at me before leaving the building and said that he would really hurt someone at Centrelink if they didn't restore his payments today. He then punched a hole in the wall. Contacted local Services Australia office (Centrelink) to warn them of the threat made by Participant 1. Site Manager arranged for the wall to be repaired. Post-incident contact was made with the Participant to discuss their behaviour'.	Actual	Abuse Behaviour Property	No	No
'Participant 2 came in and saw an EC to discuss attending a program. I overheard Participant 2 start to raise his voice at the EC. I went over to support the EC. Participant 2 looked at me and told me to 'piss off'. I explained I was there to support EC. Participant 2 started yelling and told the EC he would 'smash her head in, the	Actual Threat - Provider	Abuse Behaviour Assault no-weapon	No	No

next time he sees her'. Participant 2 was asked to leave the premises. All impacted staff were offered Employment Assistance Program. Post-incident contact was made with the Participant to discuss their behaviour'.				
'Participant 3 ran into the office with some papers. He scrunched them up and threw them into my face. 'There you go *******' he said. He kicked the door on the way out causing it to smash. Participant 3 is on an MSP & knows he can't attend the office. Provider contacted Police. All impacted staff were offered Employment Assistance Program. Site Manager arranged for the door to be repaired. Post-incident contact made with Provider to discuss their behaviour'.	Actual	Abuse Behaviour Assault weapon	Yes Police	Yes Non-compliance with restriction

- Based on information recorded in an Incident Report, the Incident Severity Matrix will automatically assign one of 3 severity levels:
  - **Low Severity**: An incident or behaviour that is a low risk to the life, health or safety of an individual or to property. The Provider may issue a verbal warning or a warning letter.
  - **Moderate Severity**: An incident or behaviour that is a moderate risk to the life, health or safety of an individual or to property. Incident requires follow-up and may require escalation. An MSP should be considered.
  - **Serious Severity**: An incident or behaviour that is a serious risk to the life, health or safety of an individual or to property. Incident requires follow-up and must be escalated to the Employment Region Lead if there is a Temporary Site Closure (see Temporary Site Closures advice on the Provider Portal). An MSP, including restrictions on access to services, must be considered.

The above incident severity levels are the same for Services Australia and Provider-lodged Incident Reports.

Please note: behaviours do not increase the severity of an incident in isolation. An additional action increases the severity of an incident i.e. the emergency services are contacted and/or the site safety impacted.

- An Incident Report Alert will appear in the top right-hand corner of a Participant's record in the Department's IT Systems, where an Incident Report has been recorded against the Participant in the previous 24 months. The alert displays the number of active Incident Reports to provide a visual indicator of potential risk.

Providers can view the number of active Incident Report/s and Services Australia incident reports for a Participant registered with them, under the incident report screen. Providers will be able to view the date of the incident and severity level.

5.5. Post-incident servicing

The challenging behaviour post-incident servicing arrangements detailed in this section have been established for Providers delivering the following programs:

- Workforce Australia Services
- Workforce Australia - Transition to Work Services
- Self-Employment Assistance
- ParentsNext
- Norfolk Island
- Yarrabah Employment Services
- Broome Employment Services

5.5.1. Post Incident Contact

The Department recommends that Providers initiate a post-incident contact with the Participant via telephone following serious challenging behaviours incidents to discuss their behaviours and the impacts those behaviours had on other Participants and staff. The purpose of a post-incident contact is to provide the Participant with an opportunity to debrief and for both the Participant and Provider staff member to gain a clearer understanding of the issues triggering the behaviours and other factors contributing to the incident (personal circumstances, barriers, and vulnerabilities, etc).

A post-incident contact should support Providers to understand whether an incident was a one-off event, or if there are ongoing factors that warrant the implementation of a Managed Service Plan (MSP) with service channel restrictions and servicing strategies to address the underlying issues impacting their behaviour.

Where either ongoing factors, or a change of circumstances are identified through the post-incident contact, we recommend the Provider consider undertaking a Change of Circumstance Reassessment through the Job Seeker Snapshot (see Chapter 4 – Job Seeker Assessments of the Workforce Australia Guidelines - Part B: Workforce Australia Services or refer to the relevant Participant assessment processes for your program).

5.5.2. Managed Service Plans (MSPs)

MSPs are arrangements that Providers can put in place to tailor the way Services are delivered to Participants who display challenging behaviours including:

- using Servicing Strategies to assist in addressing any barriers or personal circumstances contributing to behaviour, and/or
- applying Service Channel Restrictions to assist in managing the impact of behaviour.

MSPs prioritise the safety of staff and Participants while ensuring Participants stay connected to employment services and, where applicable, are able to meet their Mutual Obligation Requirements.

An MSP can be applied at any time where it is considered by the Provider to be appropriate.

Consideration of the contributing factors/barriers should be explored before Providers consider applying servicing restrictions through an MSP. Examples of factors that Providers could consider include:

- any Participant history, for example, a death in the family, carer's responsibilities, mental health issues (past or present), and drug or alcohol dependencies (past or present), and
- whether the Participant has disclosed information or displays/has previously displayed behaviour that may warrant:
    - conducting a Change of Circumstances Reassessment (CoCR) using the Job Seeker Snapshot; or
    - requesting the Participant to conduct a CoCR using the Job Seeker Snapshot.

If the Provider is unable to conduct a CoCR, they should discuss the issue with their Provider Lead.

All MSP arrangements must ensure that the Participant remains connected to employment services to meet their Mutual Obligations Requirements.

The Provider should ensure that the Participant understands the requirements of the MSP arrangements.

Some programs have been designed around more intensive and shorter servicing periods and support for their Participants. Providers should follow the relevant processes for their program.

Key steps before applying an MSP

Following an incident or change in behaviour, the Provider should, where possible, discuss the Participant's behaviour with them and, where appropriate, warn them of the implications of that behaviour. This will ensure the Participant is given the opportunity to:

- improve their behaviour, and
- disclose any contributing barriers or personal circumstances.



Warnings can be given verbally or in writing. Where a warning is given, it must be recorded on the Participant's record in Department's IT Systems, under the comments screen or in the free text section of the Incident Report where the warning was a result of an incident.

Before the Provider decides whether to apply an MSP, including the timeframe and type of MSP, they should consider:

- the severity of the behaviour and/or incident(s) including any safety concerns the behaviour may raise
- any contributing factors including barriers or personal circumstances
- the time needed to address issues (e.g. a Participant may only require a short 'cooling off' period), and
- the importance of ensuring Participants remain connected to employment services (see General Considerations).

Types of MSPs

There are 2 types of MSP:

- **Reactive** – following a challenging behaviour incident (an MSP becomes reactive once it is linked to an Incident Report in the Department's IT Systems).
- **Proactive** – where there has not been an incident but the Provider assesses a change in a Participant's behaviour and has identified barriers or personal circumstances that may increase the risk of an incident. An example of a Proactive MSP might be where a Participant has presented to a Provider Site intoxicated on several occasions, without causing any

incident. While an incident has not occurred, the Provider might assess that there is a risk of one occurring in the future and, as such, may put a Proactive MSP in place.

MSP timeframes

When applying an MSP, Providers should consider a timeframe that is appropriate to the severity of the Participant's behaviour and/or incident(s). For example:

A short-term MSP (up to one month) can be used:

- as an immediate response following an incident to provide a 'cooling off' period, or
- to allow the Provider time to further consider contributing personal factors (see General Considerations) or any other circumstances on the day e.g. physical environment, staffing etc.
- to allow the Provider time to determine if a longer-term MSP is necessary and communicate with the Participant.

A long-term (i.e. greater than one month and up to 12 months), allows time for the Provider to assist the Participant to address any barriers or personal circumstances, provide support and manage interactions between the Provider and the Participant to ensure the safety of all involved.

A long-term MSP may be extended past 12 months if, after a review, it is still necessary to support the Participant to address the causes of their challenging behaviours and to manage risks to people and property arising from the challenging behaviours. Given the extended period, the review should take into account the known drivers of the Participant's behaviours and the servicing strategies taken (and available but yet to be taken) to better identify and address issues and escalate to the Department as necessary.

An MSP must be reviewed if there are significant changes in the Participant's circumstances and if further incidents occur. At a minimum, an MSP must be reviewed twice per year.

The review of an MSP should also assess the suitability of transitioning the Participant back to standard service channels.

Servicing Strategies

The types of Servicing Strategies used are at the discretion of the Provider and should, where possible, be discussed with the Participant prior to being put in place. This is to ensure strategies are appropriate to the circumstances and proportionate to the behaviour and risk.

Providers can put in place the following Servicing Strategies (at least one Servicing Strategy is encouraged when implementing an MSP).

Table 5-C: Servicing Strategies

Strategy	Description
Anger Management Counselling	This can include general counselling.
Change of Circumstances Reassessment (CoCR)	A reassessment of a Participant's level of disadvantage, using the Job Seeker Snapshot, which may inform if a Participant requires a Job Capacity Assessment (JCA) or Employment Services Assessment (ESAt).
Financial Planning	Referral to assistance with financial planning.
Housing/Accommodation	Referral for housing/accommodation assistance.
Legal Aid	Referral to legal aid.
Welfare Agency	Referral to a welfare agency including, but not limited to, drug and alcohol counselling, grief counselling, social or community program/course or family relationship counselling.

Providers may also consider the single point servicing using the One Main Contact details provided in the One Main Contact section below.

Internal referral

As part of the MSP, the Provider should consider whether the Participant would benefit from other internal services they might offer such as counselling. They should also check with the Participant to see if their circumstances have changed and if appropriate, update a Participant's Job Seeker Snapshot or request that the Participant update their Job Seeker Snapshot.

External referral

As part of the MSP, the Provider should consider whether the Participant would benefit from other external services. This could include referral for an ESAt or JCA to ensure the Participant has been referred to the appropriate employment pathway or referral to a range of services, including but not limited to, counselling services (if not available internally), housing assistance, crisis assistance, drug and alcohol rehabilitation or legal aid.

If the Provider is unable to refer the Participant for an ESAt or JCA, they should discuss this with their Provider Lead.

The Provider should also consider the following factors when determining the Servicing Strategies:

- if a participant indicates that they generally feel better at a particular time of day, reasonable steps should be taken to hold the interview at that time (if practicable)
- an individual could be provided with the opportunity to have a support person (such as a family member or friend) who can attend any interviews
- if the participant makes any other reasonable requests in relation to the conduct of an interview or other communications, reasonable steps should be taken to accommodate those requests, and
- an interview should not continue if the participant becomes particularly distressed.

Service Channel Restrictions

The partial or full restriction of one or more service channels may assist Providers in managing the impact of challenging behaviours by enabling them to limit a Participant's contact with them.

Please note: either face-to-face or telephone servicing must remain available, either fully or partially, at all times to ensure the Participant remains connected to employment services.

Table 5-DF: Channel Restrictions

Type	Effect
Face-to-face - available	The Participant is not restricted from face-to-face services and can therefore attend any time.
Face-to-face - partial restriction	There are limitations on how, when and where the Participant may access face-to-face services. For example, a Participant is directed to attend the Site at a particular time on a particular day.
Face-to-face - full restriction	Participant cannot attend, in person, a Site where the Provider delivers services.
Telephone - available	Participant can contact their Provider by phone at any time.
Telephone - partial restriction	There are limitations on how and when the Participant can telephone the Provider. For example, a Participant is directed to call One Main Contact only.
Telephone - full restriction	Participant cannot contact the Provider by telephone.
Writing - partial restriction	There are limitations on how the Participant can write to the Provider. For example: • the Participant is directed to write to a single specific address, or • the Participant is directed to write to their One Main Contact only.
Writing - full restriction	Participant cannot contact the Provider through any written channel (email, letter or social media).

Maintaining a verbal option with at least One Main Contact will allow the Participant to contact the Provider on the same day for issues such as needing to change the time of appointment.

An example of a combination of restrictions is where you fully restrict face-to-face servicing and in writing servicing but continue with a partial restriction of telephone servicing.

One Main Contact

As part of the MSP, a Provider may decide to nominate One Main Contact within its organisation.

- The One Main Contact should be named in the MSP and the specific details of how the Participant should contact or work with their One Main Contact should be clearly outlined.
- A back up One Main Contact should also be assigned and named in the MSP in the event the primary One Main Contact is unavailable.

Approval to apply an MSP

All MSPs require approval from a Site Manager of the Provider or equivalent and must be recorded in the Department's IT Systems.

Advising the Participant of MSP arrangements

Participants must be notified of the Servicing Strategies and Service Channel Restriction/s in writing as soon as possible after the MSP arrangements have been approved. This notification should also advise the Participant that they can request the restriction/s be reviewed at any time.

Participants can be provided a letter:

- in person, if the Participant is on site
- by postal delivery (Providers should consider registered post to ensure that they can confirm that the Participant has received the letter), or
- by email.

An example template of a letter that may be sent to a Participant is available on the Provider Portal.

Participant's request for review/appeal of an MSP

Participants can have their MSP reviewed at any time or appeal the MSP when it is applied or reviewed. Participants can request a review by their Provider or contact the Department's National Customer Service Line (NCSL) to discuss the servicing arrangements in the MSP.

The Participant should be given the opportunity to participate in the review of the MSP.

As part of the review, the Provider should work through the MSP with the Participant where possible and safe to do so. If an agreement cannot be reached, the Provider should contact its Provider Lead.

Please note: If an MSP expires, it will not be automatically renewed and the Participant will no longer have any restrictions in place.

Where necessary, Providers should discuss options with their Provider Lead to either extend the MSP (if there is a continued threat to safety) or transition the Participant off the MSP.

The outcomes of a review may be to:

- end an MSP and return a Participant to standard service channels
- extend an MSP unchanged, or
- vary the MSP arrangements and set a new review date.

Additional reviews of an MSP can be initiated where there is a request from the Participant.



The Department's IT Systems automatically populate review date/s depending on the length of the MSP. Providers can amend these dates at any time. A noticeboard message will display when a review is due.

Breach of MSP arrangements

It is considered a breach when a Participant does not follow the servicing arrangements and service channel restrictions as set out in their MSP.

Where a Participant is in breach of the MSP, the Provider must lodge an Incident Report in the Department's IT Systems.

If the Provider identifies that the Participant was not aware of the MSP or service channel restrictions (i.e. did not receive their letter) this should also be recorded in the Department's IT Systems.

Where a Participant has an MSP in place, an MSP Alert will appear in the top right-hand corner of a Participant's record in the Department's IT Systems. The alert displays:

- Service Channels and the level of restrictions, in a traffic light format
- if One Main Contact is in place, and
- if Servicing Strategies are in place.

Where a Participant repeatedly breaches their MSP and/or continues to be a threat to staff, the Provider should escalate the matter to its Provider Lead. Where necessary, the Provider Lead will refer the case to the relevant team in the National Office of the Department for review and further assistance in managing the behaviour.

Servicing Participants post MSP

Providers should consider how the Participant will be serviced when the MSP and service channel restrictions have been lifted and they return to standard servicing. Providers should record in the Participant's MSP the ongoing measures that will be implemented to encourage improved behaviour by the Participant.

5.5.3. Transfers between Providers when a Participant has a Serious Incident and/or Reactive MSP

Participants with a current Provider-lodged and/or DHS-lodged Serious Incident Report and/or Reactive MSP seeking a transfer to a different Provider may only be transferred with the involvement of the Department. For more information, Providers should refer to the relevant transfer processes for their program.

Notification of Transfers and Referrals

A system pop-up notification will be provided for all Participants with incidents and/or MSPs in the Department's IT System. These include incidents and MSPs created by Services Australia since 4 July 2022. Provider staff should review the details of historical Participant incident reports and MSPs in the IT System prior to scheduling an Initial Interview so they can implement appropriate interview safety measures to protect Participants and staff, and improve engagement. This may include implementing a proactive MSP limiting face-to-face servicing where appropriate, ensuring there are clear expectations around behaviours and a plan to move towards opening the full suite of communication channels and strategies to support the Participant to manage their behaviour.

5.5.4. Transfers Due to Relationship Failure

If a Provider thinks it cannot maintain a reasonable and constructive servicing relationship with a Participant, they can request that the Participant be transferred to another Provider for servicing.

This type of request will require the Provider to demonstrate a genuine attempt to implement post-incident servicing arrangements as outlined in this Chapter. For more information, Providers should refer to the relevant transfer processes for their program.

5.5.5. Summary of required Documentary Evidence

- Providers must use the Incident Report screen in the Department's IT Systems to record all instances where a Participant exhibits challenging behaviours.
- Any warnings given to a Participant must be recorded on the comments screen on the Participant's record in the Department's IT Systems.
- Providers must record all MSP arrangements and restriction/s that are put in place in the MSP screen on the Participant's record in the Department's IT Systems.