



Records Management, Privacy and External Systems Assurance Framework 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 2.1

Published on: 6 June 2023

Effective from: 1 July 2023

In this version of the Guideline the Privacy Chapter has been updated to reflect that consent obtained from individuals by Providers should be regularly reviewed.

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. Records Management Instructions	4
Chapter 2. Privacy	14
Chapter 3. External Systems Assurance Framework (ESAF)	27

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.

Please note: Throughout this document, text currently appears in **yellow highlight**. Text formatted in this manner indicates that the Department proposes to upload a supporting document to the Provider Portal that did not have a link available as at the published date.

Some links in this document are program-specific and may not be accessible by all Providers. Providers should note that this Guideline has been developed to align with Workforce Australia requirements where possible, however, some requirements in this Guideline differ.

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.

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

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

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

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

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

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

'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.

Chapter 1. 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 Form – Employment Services](#)
- [Records Retention Periods](#)
- [General advice on management of Records](#)
- [The Office of the Australian Information Commissioner Guide to securing personal information](#)
- [Privacy Incident Report](#)

1.1. 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.

1.2. 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.

1.2.1. 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](#).

1.3. 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, Providers must, wherever possible and consistent with the Deed and other applicable legal requirements, create and manage Records in a digital format. Physical Records created before 1 July 2023 can be retained in a physical format, unless otherwise specified by the Department, any Deeds or Guidelines and legal requirements.

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.

1.3.1. 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 breach, 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.

1.3.2. 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.

1.4. 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.

1.5. Transfer of Records

1.5.1. 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.

1.6. 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.

1.6.1. Return of Digital Records

Providers creating digital Records must use a format that is acceptable under the *Archives Act 1983* (Cth) (the *Archives Act*) and that will allow the Department to read the Records if returned to the Department in the future.

Digital Records in the Department's IT Systems or those that do not relate to the provision of Services under the Deed do not need to be returned to the Department.

Secure File Transfer Protocol (SFTP) is the Department's preferred method of transferring files on the internet or any Transmission Control Protocol/Internet Protocol network, particularly when handling large numbers of files and large files, with external parties. Refer to the [Return of Records Form – Employment Services](#) for information.

1.6.2. Return of Physical Records

Providers must obtain the Department's approval prior to returning any physical Records to the Department.

Providers must use the 'Form - Providers to complete to return of Physical Records to the Department to return Records'. Refer to the [Return of Records Form - Employment Services](#) to access this form.

1.6.3. Providers' Access to Returned Records

Where a Provider requires access to a Record that has been returned to the Department, the Provider must write to the Provider Lead with the details and purpose of the request for the Department's consideration.

Where Records have been returned to the Department and a Provider receives an order to produce documents included as part of the returned Records, such as a subpoena, the Provider may contact their Provider Lead. In these circumstances, the Provider may also seek their own independent legal advice.

1.7. 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.

1.7.1. 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 (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.

1.7.2. 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.

1.8. Breaches and Inappropriate Handling of Records

1.8.1. 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](#).

1.8.2. 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.

1.8.3. 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.

1.9. Retention of Records

All Records must be retained by the Provider for a period of no less than 7 years after the creation of the Record, unless otherwise specified in 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 supporting document [Records retention periods](#).

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.

1.9.1. 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. See more information related to Digital Records under Management of Records.

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

1.9.2. 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.

1.10. 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.

1.10.1. 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.

1.10.2. 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)

1.10.3. 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.

1.10.4. 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 2. Privacy

Supporting Documents for this Chapter:

- [Privacy Notification and Consent Form](#)
- [Provider Privacy Incident Report](#)
- [Learning Centre: Information Exchange and Privacy Module](#)

2.1. 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.

2.2. 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.

2.2.1. 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.

2.2.2. 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](#).

2.3. 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.

2.3.1. 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:

- provide and explain the [Privacy Notification and Consent Form relevant to their program \(ParentsNext and Time to Work Employment Services and Harvest Trail Services¹\)](#), 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 Forms](#). Please note Providers may digitise, but must not amend, the Privacy Notification and Consent Form, 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:

¹ The Privacy Notification and Consent Form in Harvest Trail Services is contained in the relevant Direct Registration Form. HTS Providers should refer to the [Delivering Harvest Trail Services Guidelines](#) for more information.

- 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.

2.3.2. 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.

2.4. 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.

2.5. 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.

2.6. 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 relevant 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.

2.6.1. 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.

2.6.2. 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.

2.7. 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.

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

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

APP 9 provides limited exceptions where a Provider may:

- 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.

2.9. 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.

2.9.1. 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.

2.10. 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.

2.10.1. 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.

2.10.2. 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.

2.10.3. 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). In accordance with the Class PIC, under the [Instrument of Delegation](#), the Secretary has delegated the power to disclose information 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) within the previous 12 months.

A delegate may disclose Protected Information about an individual under the Class PIC in cases:

- where the request is from police, emergency services, an emergency call service "Triple Zero", health service providers, or child protection agencies, and
- 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.

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 purpose of the disclosure is the investigation of an offence or threatened offence has occurred against an officer, or against Commonwealth property, or in premises occupied by an employment services Provider contracted to the Department.

Before disclosing the information, 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.

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.

For more information around disclosing Protected Information under the Class PIC, please refer to the [Class PIC Factsheet](#).

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 by consent of the individual. Examples include:

- releasing Protected information to Police or other authorities to assist an investigation when there is no threat to anyone's life, health or welfare; and
- responding to a subpoena or other notice requiring production of documents.

The Provider will need to approach the Department through their Provider Lead to request a specific PIC. The Provider should make the request as soon as they become aware of circumstances where they wish to, or are being asked to, disclose Protected Information, and outline the reasons why the Provider proposes to disclose the Protected Information, 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 consult their own independent legal advice before responding to the request for Protected Information.

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.

2.11. 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.

2.12. 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](#).

2.13. 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](#).

2.14. 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 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.

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.

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

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

Providers should ensure their internal privacy practices, policies and procedures are proactively reviewed, taking into account compliance with new laws or updated information handling practices, and ensuring that they are responsive to new privacy risks.

2.14.2. Personnel Compliance

Providers must monitor and annually self-audit that 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 3. External Systems Assurance Framework (ESAF)

3.1. Chapter Overview

This Chapter provides guidance for Providers in relation to:

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

under the ESAF.

Providers are able to access sensitive client information via the Department's online systems. This level of access requires appropriate levels of security.

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

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

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

3.2. External Systems Assurance Framework

The ESAF provides assurance that the risks to the Department's IT Systems and data, information and Records stored outside of the Department's IT Systems environment are managed securely and appropriately.

This is consistent with the whole of government Protective Security Policy Framework (PSPF). As part of the PSPF, the Department is accountable for ensuring that all contracted Providers used in the delivery of its programs also comply with PSPF requirements.

The ESAF covers External IT Systems associated with:

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

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

3.2.1. Providers' IT Systems

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

3.2.2. Third Party Employment Systems (TPES)

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

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

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

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

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

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

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

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

3.3. Right Fit for Risk approach

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

- **International Standard ISO/IEC 27001:2013** Information technology – Security techniques – Information security management systems – Requirements (ISO 27001) – the international standard outlining the core requirements of an Information Security Management System.
- **Australian Government Information Security Manual (ISM)** – the Australian Government's cyber security framework to protect systems and data from cyber threats.

The RFFR approach includes a requirement that Providers design and implement an Information Security Management System (**ISMS**) that is consistent with the requirements of ISO 27001. An ISMS

is a systematic approach to managing business information so that it remains secure and available when staff need it. It secures people, premises, IT systems and information by applying a risk management process to information security.

The RFFR program extends ISO 27001 in 2 key areas:

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

3.4. Guidelines for accreditation and maintenance of accreditation

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

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

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

3.5. Provider classification for accreditation

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

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

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

- IT environment
- level of outsourcing
- subcontracting arrangements
- organisational structure
- level of security maturity
- the extent of sensitive information held and level of access to departmental systems
- other relevant factors.

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

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

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

Table 3-A provides guidance to Providers on the basis of accreditation and accreditation maintenance activities required for each category.

Table 3-A: Provider Classification

Category	Category 1	Category 2	
Sub-category	Nil	2A	2B
Annual Case load	2,000 or more	Under 2,000	Under 2,000
Risk profile	Greater risk	Medium Risk	Low risk
Basis of accreditation	ISO 27001 conforming ISMS - independently certified	ISO 27001 conforming ISMS - self-assessed	Management Assertion Letter
Accreditation maintenance	Annual surveillance audit and triennial recertification	Annual self-assessment	Annual management assertion letter
Milestones to complete	1, 2 and 3	1,2 and 3	1 and 3

3.6. Milestones for completing the accreditation process

3.6.1. Milestone 1

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

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

Table 3-B sets out the requirements for Milestone 1 for Providers who are already accredited or already in the process of being accredited.

Table 3-B: Requirements for the Milestone 1 process

Assessment method	Review of submitted RFFR questionnaire and discussion.
Submission deliverables	RFFR questionnaire submitted by the Provider as part of their RFP/RFT response.
Key actions and outcomes	<p>The Provider and Department representatives will discuss the Provider’s business, stakeholders, contractual obligations, information, systems and practices to assist the Provider to determine the scope of their Information Security Management System.</p> <p>Unaccredited Providers: The Department will confirm the Provider’s categorisation and the associated RFFR assurance requirements for completing Milestone 2 and 3. Providers intending to deliver Services to fewer than 2,000 individuals will review additional risk factors with the Department to determine whether the Provider should be classified into Category 2A or 2B.</p> <p>Providers part way through an existing accreditation process: Existing Providers who are part way through an accreditation process for delivering Services under an existing Employment Deed should take steps as advised in the purchasing documentation.</p> <p>Accredited Providers with new Deeds: The Department will review the extent of changes to the Provider’s scope of Services and determine if the Provider should be in a different category as a result of the new Deeds. In accordance with the terms of their accreditation, the Provider should consider whether their Information Security Management System requires review and update to ensure that people, locations, systems and information associated with services under the new Deeds are appropriately secured; and notify the Department. If no significant changes have occurred, accredited Providers do not need to complete Milestones 2 and 3 and need only maintain their RFFR accreditation.</p>
Next steps	<p>For large organisations it is recommended Providers appoint a champion within the organisation to ensure compliance with the RFFR</p> <p>Commence development of documentation required by the Provider’s category (see Table 3-C below)</p> <p>Identify where existing security controls meet RFFR requirements, and where there are gaps requiring that additional controls be implemented.</p>
Due dates	Completed within one month of Deed execution by the Department.

3.6.2. Milestone 2

Milestone 2 requires Providers to demonstrate their ISMS has been designed to reflect RFFR requirements applicable for their Category (as advised at Milestone 1). Providers are required to

demonstrate that appropriate security controls are planned to be implemented within the organisation through submission of required documentation.

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

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

Table 3-C lists the requirements for Providers to achieve Milestone 2.

Table 3-C: Milestone 2 requirements

	Category 1 Provider	Category 2A Provider	Category 2B Provider
Submission deliverables	<ul style="list-style-type: none"> ISMS scope Statement of Applicability (SoA) reflecting RFFR requirements Independent assessor’s Stage 1 report 	<ul style="list-style-type: none"> ISMS scope SoA reflecting RFFR requirements ISMS Self-assessment report (conformance) 	Not applicable
Implementation status	Provider’s ISMS is expected to substantially conform with ISO 27001 requirements, however applicable controls sourced from ISO 27001 Annex A and from the Australian Government Information Security Manual are not expected to be implemented at this stage		
Assessment method	Independently issued assessed by a JAS-ANZ accredited ISO 27001 conformance assessment body	Self-assessed by business owners	
Outcomes to progress to Milestone 3	Department acceptance of submission deliverables.	Department acceptance of submission deliverables.	
Next steps	Implement the ISMS in accordance with its design		
Due dates	To be completed within 3 months from the Deed Commencement Date		

3.6.3. Milestone 3

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

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

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

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

Table 3-D: Milestone 3 requirements

	Category 1 Provider	Category 2A Provider	Category 2B Provider
Submission deliverables	<ul style="list-style-type: none"> Updated SoA identifying the current implementation status of applicable controls, and the applicability decision for new or changed controls published since the SoA’s last review Independent assessor’s “Stage 2” report attesting to the ISMS conformance with ISO 27001 and the status of all applicable controls in the Provider’s customised SoA ISO 27001 or DESE ISMS Certificate (when available) 	<ul style="list-style-type: none"> Updated SoA identifying the current implementation status of applicable controls, and the applicability decision for new or changed controls published since the SoA’s last review ISMS self-assessment report (implementation) 	Management Assertion Letter
Implementation status	Provider’s ISMS conforms with ISO 27001 and controls applicable to the organisation have been implemented		Controls supporting specific security objectives have been implemented
Assessment method	Independently assessed	Self-assessed	Self-assessed
Outcomes to complete process	<ul style="list-style-type: none"> Department acceptance of submission deliverables RFFR accreditation 		

	Category 1 Provider	Category 2A Provider	Category 2B Provider
Next steps	<ul style="list-style-type: none"> Address any remaining minor non-conformances Implement remaining applicable controls (if any) Monitor the ISMS 		Monitor performance of security controls
Due dates	To be completed within 9 months from the Deed Commencement Date		To be completed within 9 months from the Deed Commencement Date

3.7. Submission deliverables

3.7.1. Submission milestones

Table 3-E below provides a high-level description of the deliverables that need to be submitted to the Department as part of the accreditation process. The Department does not require the use of any specific template, except for the RFFR questionnaire completed for Milestone 1 as part of the Provider’s RFT/RFP response. Standard templates for each deliverable are available from the Department and may be optionally used as a basis for working through the accreditation process.

Each of the submission deliverables in Table 3-E is described in more detail in Table 3-F.

Table 3-E: Provider Milestones Deliverables

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

3.7.2. Deliverable descriptions

Table 3-F below provides a detailed description of, and criteria for completing, each deliverable of the RFFR process.

Table 3-F: Deliverable descriptions

Submission Document	Description
RFFR questionnaire	Submitted with the Provider’s RFT/RFP response where required, the questionnaire seeks information regarding the Provider’s business, their IT security posture and their readiness to meet RFFR requirements. Discussing the completed questionnaire with the Department marks completion of Milestone 1 and confirms the Provider’s category.
ISMS scope document	The purpose of this document is to clearly define the boundaries of the ISMS to provide the Department with an understanding of the Provider’s business and context, in conformance with ISO 27001 Clause 4. It should also provide a high-level description of how the Provider intends to meet RFFR core expectation areas. A template scope document is available from the Department.
Statement of Applicability (SoA)	<p>The SoA demonstrates the Provider’s consideration of each of the security controls sourced from ISO 27001’s Annex A and ISM’s OFFICIAL security controls and the determination of which controls will form part of the Provider’s ISMS. It also communicates the rationale for determining that individual controls are “not applicable” to the Provider’s business.</p> <p>For applicable controls, the SoA should indicate relevant policies/procedures or other documentation demonstrating that the control has been included in the Provider’s business and should indicate the current implementation status of each applicable control.</p> <p>The SoA is a mandatory artefact required to conform with ISO 27001 Clause 6. An ISO to ISM controls mapping document is available from the Department to assist with developing the SoA.</p>
Independent assessor’s “stage 1” report	For Category 1 Providers (or other Providers who see benefit in obtaining an industry certification). This is the first of 2 independent assessments required to achieve ISO 27001 or DESE ISMS Scheme certification. Performed by a JAS-ANZ registered certification assessment body, the stage 1 report verifies the extent to which the Provider’s ISMS has been designed to conform with the requirements of ISO 27001 and identifies design gaps to be addressed prior to commencing the stage 2 assessment. Because RFFR requires a customised SoA it is critical that the report states that the assessment was performed over the ISMS as described by that customised SoA – with a clear report reference to the SoA by version/ date.
Independent assessor’s	For Category 1 Providers (or other Providers who see benefit in obtaining an industry certification). This is the second of 2 independent assessments required to achieve ISO 27001 or DESE ISMS Scheme certification and is a key source of

Submission Document	Description
“stage 2” report	<p>assurance that the Provider has implemented the controls identified as applicable in the SoA. Performed by a JAS-ANZ registered certification assessment body, the stage 2 report validates that the implemented ISMS conforms with the requirements of ISO 27001 and that applicable controls are in place and operating.</p> <p>Because RFFR requires a customised SoA it is critical that the report states that the assessment was performed over the ISMS as described by that customised SoA – with a clear report reference to the SoA by version/ date - and that the report provides information regarding the status of both Annex A- and ISM-sourced applicable controls (particularly applicable controls that support RFFR core expectation areas - see section 4.9).</p>
ISO 27001 certificate or DESE ISMS Scheme certificate	<p>Issued after the Provider has demonstrated plans to address any non-conformances identified in the stage 2 report and the independent assessor has recommended the Provider for certification. The DESE ISMS Scheme certificate is an adaptation of the ISO 27001 certificate designed to demonstrate that RFFR requirements have been met.</p>
ISMS Self-Assessment report	<p>For Category 2A Providers only, the self-assessment report is the Department’s source of assurance that the ISMS described by the Provider’s SoA has been designed (for Milestone 2) and implemented (for Milestone 3) in accordance with ISO 27001 and RFFR requirements.</p> <p>It is critical that the self-assessment report be signed off by a person/s with appropriate authority to make declarations on behalf of the Provider, that it attest to the Provider’s ISMS conformance with ISO 27001 requirements, and (for Milestone 3) that it attest to the implementation status of controls identified as applicable in the Provider’s SoA. A template self-assessment report is available from the Department.</p>
Management Assertion Letter	<p>For Category 2B Providers only, the Management Assertion Letter is the Department’s source of assurance that the Provider represents minimal risk and has implemented security controls that respond to relevant security objectives. The letter covers a description of the Provider’s systems and controls, attests that the description is accurate and that the described controls are appropriate to meet specific security objectives.</p>

3.7.3. Considerations for accreditation commencement

Table 3-G provides guidance to Category 1, 2A and 2B Providers on areas of focus to consider before commencing the RFFR accreditation process.

Table 3-G: Considerations for accreditation commencement

Area	Description
Sponsor	Identify a sponsor within the organisation to support the RFFR certification process. The sponsor will help guide and support the accreditation process, including ensuring that appropriate resources are available to complete RFFR accreditation.
Scope	Determine the scope of the ISMS. Consider the organisational context and business activities performed at each site, stakeholders and their needs, physical boundaries, legal and contractual requirements, and logical boundaries (systems and data). The scope should communicate key aspects of the Provider’s business, the importance of security and state what the ISMS will be protecting.
Gap Analysis	Before the Milestone 2 submission, Providers should perform an initial review and gap assessment to identify areas of current conformance with ISO 27001 and areas requiring future focus. The gap assessment should also identify if the Provider already has some applicable controls in place and which require action to implement. As a management review of the ISMS, this assessment is itself a requirement of ISO 27001. Performing the gap assessment prior to Milestone 2 will ensure time to address non-conformances and to plan improvements before the Provider’s final submission.
Certifying Assessment Body	For Category 1 Providers (or other Providers who see benefit in obtaining an industry certification), identify a suitable Certifying Assessment Body (CAB) to work with your organisation to provide the independent assessments required under the ISO 27001 requirements (see 4.7.4 below).

3.7.4. Certifying Assessment Bodies

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

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

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

3.8. Accreditation maintenance

During the lifespan of their Employment Deed/s, Providers are required to maintain their RFFR accreditation status through annual reporting (each financial year) and surveillance audits to ensure

compliance to the standards (see [Table 3-H](#) below). Providers with an existing accreditation will need to complete the annual and 3 yearly audits based on the dates when the accreditation was granted.

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

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

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

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

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

Table 3-H: Ongoing accreditation requirements

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

3.9. Core expectations of Providers under the RFFR

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

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

Providers should implement controls for:

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

Providers should implement security controls that are responsive to:

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

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

3.9.1. RFFR Core Expectations: Personnel security

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

- identify the individual and positively confirm the individual's identity
- verify the competency of the individual by verifying qualifications, certifications and experience provided on their CV
- obtain a satisfactory police check for the individual
- satisfactorily complete Working with Vulnerable People checks as required by individual states / territories
- confirm the individual has a valid right to work in Australia – a person who is not an Australian citizen must hold appropriate work entitlements
- verify that the individual has successfully completed initial and ongoing security awareness training programs with content and timing tailored to their role
- execute employment contracts which state that responsibilities for information security and non-disclosure requirements continue post termination

- implement higher levels of assurance for individuals that have privileged or administrative level access. The additional Personnel expectations include that individuals must be Australian citizens or permanent residents to give them sufficient connection with Australia and be willing and able to undertake a suitability background check.

3.9.2. RFFR Core Expectations: Physical security

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

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

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

3.9.3. Essential Eight cyber security strategies

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

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

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

Table 3-I: Essential Eight cyber security strategies

Control	Description
Application Control	to control the execution of unauthorised software. This prevents unknown and potentially malicious programs executing in your environment.
Patch Applications	to remediate known security vulnerabilities in application software. Security vulnerabilities in applications can be used to execute malicious code. Using the latest version of applications and promptly applying patches when vulnerabilities have been identified will keep your environment robust.
Configure Microsoft Office macro settings	to block untrusted macros. Microsoft Office macros can be used to deliver and execute malicious code. This strategy will only allow macros from trusted locations with limited write access, or those digitally signed with a trusted certificate, to run.

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

3.10. General requirements

3.10.1. Security Contact

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

3.10.2. Subcontractor and Third Party IT Vendor requirements

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

The Provider must:

- ensure that its Subcontractors successfully complete the required Personnel vetting processes, and bear any costs associated with doing so.
- ensure that its Subcontractors and its Third Party IT Vendors are aware of, and comply with, the same security requirements that are placed on the Provider by the Department. This includes consideration and implementation of ISM OFFICIAL controls that are relevant to the scope of services provided by the Subcontractor or Third Party IT service provider.

3.10.3. Access and information security assurance for External IT Systems

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

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

3.10.4. Cloud Services Providers

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

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

3.10.5. Breaches of security requirements

Where the Department considers that the Provider has breached their Employment Deed, including RFFR or security requirements, or there is a risk of such a breach, the Department may immediately suspend Access, or require the Provider to cease all Access, to the Department's IT Systems. Where the Department determines that the Provider is in breach of, or has previously breached, relevant

requirements, the Department may immediately take action including any one or more of the following:

- suspending, terminating, or requiring the cessation of all access to the Department's IT Systems for any Provider Personnel, Subcontractor, Third Party IT Vendor, External IT System or the Provider;
- requiring the Provider to obtain new logon IDs for any Provider Personnel, Subcontractor or Third Party IT Vendor and, if so required, the Provider must promptly obtain such new logons; or
- requiring the Provider to prepare and implement an IT security plan to the Department's satisfaction, and if so required, the Provider must do so within the timeframe required by the Department.

