Australian Government

Disability Employment Services

Records Management Instructions Guidelines V1.1

Disclaimer
This document is not a stand-alone document and does not contain the entirety of Disability Employment Services Providers' obligations. It should be read in conjunction with the Disability Employment Services Grant Agreement and any relevant guidelines or reference material issued by the Department of Social Services under or in connection with the Disability Employment Services Grant Agreement.

Table of Contents

Records Management Instructions Guidelines

Document Change History

Version	Start Date	Effective Date	End Date	Change and Location
1.1		19 February 2021		Submit completed PIR within 15 business days.
1.1		19 February 2021		*Attachment A* – NEW two stage Provider Incident Report (PIR)
1.1		19 February 2021		Change Account Manager to Relationship Manager
1.0		1 Jul 2018		Original version of document

Summary

The Records Management Instructions (RMI) Guidelines covers Disability Employment Services (DES) Program Providers (hereon referred to as 'Providers') management of identified Agreement Records and includes minimum retention periods under two broad categories:

- Records with retention periods of 6 years ('Priority Records')
- Records with retention periods of 3 years ('General Services Records')

The full description of RMI Records is available at in *Attachment C: Records Retention Periods*.

The RMI provide legally binding instructions for the management, retention and disposal of identified Records created or used by Providers during the delivery of Services under the Disability Employment Services Grant Agreement ('the Agreement') for the Department of Social Services ('the department'). Providers should read the RMI in conjunction with applicable provisions of the Agreement.

Except as provided for in the next sentence, inactive Records involving Participants under previous contractual arrangements (i.e. prior to the current Agreement) are not included in these RMI and Providers are required to manage these Records in accordance with arrangements in place at that time. The option for Providers to convert paper Records to electronic format as provided at *Section 3: Agreement Records* of these RMI applies to any paper Records created after 1 January 1995, including those created under previous contractual arrangements.

1. Relevant Agreement Definitions

The Department of Social Services (DSS) administers the DES Program. All references to 'DSS' in the Agreement and any Guidelines, including the definitions extrapolated from the Agreement below, are to be read as references to the 'department'.

'**Agreement Material**' means all Material:
(a) created for the purpose of performing the Agreement;
(b) incorporated in, supplied or required to be supplied along with the Material referred to in paragraph (a) above; or
(c) copied or derived from Material referred to in paragraphs (a) or (b); and
(d) includes all Agreement Records.

'**Agreement Records**' means all Records:
(a) created for the purpose of performing the Agreement;
(b) incorporated in, supplied or required to be supplied along with the Records referred to in paragraph (a) above; or
(c) copied or derived from Records referred to in paragraphs (a) or (b); and
(d) includes all Reports.

'Commonwealth Material' means any Material provided by the department to the Provider for the purposes of the Agreement and Material which is copied or derived from Material so provided, and includes Commonwealth Records.
'Commonwealth Records' means any Records provided by the department to the Provider for the purposes of the Agreement, and includes Records which are copied or derived from Records so provided.

'Department's IT Systems' means the IT computer system accessible by a Provider, through which information is exchanged between the Provider, Subcontractors, DHS, DHS Assessment Services, Ongoing Support Assessors and the Department in relation to the Services.

'Documentary Evidence' means those Records of the Provider, as specified in the Agreement including in any Guidelines, which evidence that Services were provided by the Provider for each claim for payment made under the Agreement, or which otherwise support a claim for payment by the Provider.

'**Material**' includes equipment, software (including source code and object code), goods, and Records stored by any means including all copies and extracts of the same.

'**Participant Services Records**' means Agreement Records (including documents associated with the Customer Feedback Register) about a Participant that are directly created for the purposes of providing Services.

'**Provider Records**' means all Records, except Commonwealth Records, in existence prior to the Agreement Commencement Date:
(a) incorporated in;
(b) supplied with, or as part of; or
(c) required to be supplied with, or as part of,
the Agreement Records.

'**Records**' means documents, information and data stored by any means and all copies and extracts of the same, and includes Agreement Records, Commonwealth Records and Provider Records.

Notes:
It is important to note that the department owns the Commonwealth Material and Agreement Material but grants the Provider a licence to use, copy and reproduce it for the purposes of the Agreement and in accordance with any conditions or restrictions Notified by the department to the Provider.

The term 'Commonwealth Records' is used above and throughout this document in a manner that is different to how the term is defined in the *Archives Act 1983*. Under the Archives Act, 'Commonwealth records' are not just those records that are provided by the Commonwealth to the Provider, but rather all records that are the property of the Commonwealth i.e. 'Commonwealth Material' and 'Agreement Material'. This distinction is relevant to the permission granted by National Archives of Australia for the destruction of Commonwealth records where those records have been converted from hard copy to electronic form (see *Section 3: Agreement Records*).

Explanatory Notes:
- Unless the contrary intention appears, all capitalised terms have the same meaning as in the Agreement.
- 'Must' indicates that compliance is mandatory; 'should' means that compliance represents best practice.

These Guidelines should not be read as a stand-alone document. Please refer to the Disability Employment Services Grant Agreement and the National Panel of Assessors Program Grant Agreement.

2. Records Framework

Records can generally be separated into three groups:

- ***Commonwealth Records*** – includes Records provided by the department to Providers such as the Employment Pathway Plan template or information about a Participant;
- ***Agreement Records*** – includes Records created during the course of providing Services such as Participant Services Records and the Customer Feedback Register; and
- ***Provider Records*** – includes Records in existence prior to the Agreement commencing except for any Commonwealth Records.

The RMI cover only those Records identified in *Attachment C: Records Retention Periods*, wherever they are held in the Provider organisation.

Commonwealth Material (which includes Commonwealth Records) and Agreement Material (which includes Agreement Records) are owned by the department. Providers have no requirements other than what is specified in the Agreement in relation to Commonwealth Material and Agreement Material.

3. Agreement Records

Providers must create accurate Records (including, for example, Participant Services Records) in the course of delivering employment Services. Subject to certain exclusions and conditions, Providers may convert paper Records created on or after 1 January 1995 to electronic form and destroy the originals.

3.1 Requirements

Providers may create Records in either paper or electronic form. Arrangements outlined in the RMI cover both forms of a Record. Consistent with the department's record keeping policy, it is preferred that all Records are created and managed electronically. This is in line with the whole-of-government approach to digital information known as the Digital Continuity 2020 Policy. This policy covers all government information, data and records, as well as systems, services and processes, including those created or delivered by third parties on behalf of Australian Government agencies.

Records that are created electronically should be maintained in digital format. This will ensure that the requirements of the *Electronic Transactions Act 1999* (Cth), and the Agreement are met. Subject to this Section 3, Providers can retain Records in a manner which suits their own business arrangements.

All Commonwealth Material and Agreement Material are 'Commonwealth records' as defined under the *Archives Act 1983* (i.e. records that are the property of the Commonwealth). Subject to certain exclusions and conditions, National Archives provides permission for the destruction of Commonwealth records created on or after 1 January 1995 under General Records Authorisation 31 (GRA-31) where those records have been converted from hard copy to electronic form. GRA-31 applies to Providers as 'authorised agents' of the department. Providers must comply with the requirements of GRA-31. For convenience, the relevant exclusions and conditions are set out below.

3.1.1 Exclusions

GRA-31 does not cover the destruction of records that have been reproduced where:

(a) the Provider considers the record to have intrinsic value in its original format or a specific format and it is identified by National Archives of Australia as:
  (i) Retain as National Archives (RNA); or
  (ii) Retain Permanently (RP); or
  (iii) meeting the criteria for RNA listed in 'Why Records are Kept: Directions in Appraisal';

(b) the record is an audio visual record that has not been identified as a temporary record under a current Records Authority issued by the National Archives of Australia;

(c) there is a legal requirement to retain the record in its original format or a specific format;

(d) there is a government policy or directive not to destroy the record (e.g. the record is the subject of a *current disposal freeze*, as advised by National Archives of Australia) such as the institutional responses to child sexual abuse;

(e) the Provider knows it is reasonably likely that the record may be required as evidence in:
    (i) a current judicial proceeding; or
    (ii) a future judicial proceeding that will be commenced or will likely be commenced;
(f) the record is subject to a current application for access under the *Freedom of Information Act 1982*, the *Archives Act 1983* or other legislation;
(g) the National Archives of Australia has issued a notice that specifically prohibits destruction of the record; and
(h) the National Archives of Australia has issued a notice that specifically requires retention of the record in its original format or a specific format.

3.1.2 Conditions

(a) Providers must ensure that all reproductions are at least functionally equivalent to the source records for business and legal purposes and are managed as official agency records (principally, this means that Providers' electronic records management systems must be such that they, and the department, can be satisfied that the reproduction is:
    (i) authentic – the reproduction process is controlled and documented;
    (ii) complete – the reproduction has been produced using quality assurance measures that ensure there is no alteration, and has all the information as contained in the source record;
    (iii) accessible – the reproduction is available and readable over the life of the record; and
    (iv) useable – the reproduction is able to serve the same business purpose as the source record.
(b) Prior to the destruction of source records, Providers must conduct a risk assessment of the likelihood that the records may be required as evidence in:
    (i) a current judicial proceeding or future judicial proceeding that will be commenced or will likely be commenced; or
    (ii) are the subject of a current application for access under the *Freedom of Information Act 1982*, the *Archives Act 1983* or other legislation.

    Where the Provider determines that the source records are reasonably likely to be required, the source records must not be destroyed until after the judicial proceeding or application for access has been finalised.
(c) Where GRA-31 permits the destruction of original records after digitisation or other copying, the date a copy record or a subsequent copy record came into existence is taken to be the date that the original record came into existence. Therefore Providers must, in creating an electronic copy of a document, note and record the date on which the original copy was created.
(d) Providers must ensure that the reproductions are maintained for as long as required by Employment Services Records Authority 2009/00179260 (see *Attachment C: Records Retention Periods*).

Further explanation of the relevant exclusions and conditions is provided in the *Guidelines for using General Records Authority 31* issued by the National Archives of Australia. Providers must have regard to these Guidelines in developing any practices and policies for converting paper-based Records into electronic format and, after doing so, in relation to the destruction of the original paper-based Records.

Providers will need to provide access to electronic Records if requested by the department under the Agreement. For example, Providers must provide direct access to electronic Records in a Provider database or print copies of appropriate screens, if requested by the department.

Records scanned into an electronic system must also be retained in accordance with the RMI. That is, the scanned information must be retained in accordance with appropriate retention periods.

Information in the department's IT Systems is an important source of Participant information and will be retained by the department for the appropriate retention periods.

Refer to *Section 9: Return of Records* for more information on electronic Records.

4. Storage of Documentary Evidence in the Department's IT systems

From 1 July 2018 Providers must, at the time a claim for a payment is made, upload to the Department's IT Systems the Documentary Evidence referred to in clause 22.1 of the DES 2018 Grant Agreement as required by any Guidelines, to the Department's satisfaction.

Providers must if requested by the Department, within 10 Business Days of the Department's request, provide to the Department any Documentary Evidence referred to in clause 22.1 that was not uploaded to the Department's IT Systems in accordance with clause 22.2, to the Department's satisfaction.

THE FOLLOWING INFORMATION APPLIES TO ALL RECORDS THAT ARE NOT REQUIRED TO BE STORED IN THE DEPARTMENT'S IT SYSTEMS, AS PART OF THE REQUIREMENTS OUTLINED AT SECTION 4 ABOVE.

5. Records Storage

Providers must securely store all Records appropriately both on and off-site. All incidents involving inappropriate access, damage, destruction or loss of Records must be reported to the department, to ensure compliance with legislation.

Providers must not transfer Personal Information outside Australia, or allow parties outside Australia to have access to it, without the prior written approval of the department.

5.1 General Storage Requirements

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/Agreement Records, for example, the *Privacy Act 1988* outlines arrangements for the management of Personal Information. In addition, Providers are required to store Records in accordance with the department's Security Policies, including *the External Security Policy – For Contracted Service Providers and Users*, available on the IT Security & Access page on the Provider Portal (DES > Provider Operations > IT Security & Access). Providers must ensure the department has access to Records if required, either by providing access to a storage facility or by retrieving the Record (including if stored electronically by retrieving the electronic copy and if relevant printing it) and providing it to the department.

Providers must ensure Records are protected from:

- storage environment damage (e.g. paper Records damp from cement floor)
- unauthorised alteration or removal
- use outside the terms of the Agreement
- breaches of privacy, particularly in relation to Participant Records
- inappropriate 'browsing' of Records by Provider staff or any other person.

Records containing sensitive information as defined in the *Privacy Act 1988*, such as police checks or medical information, must be kept in lockable cabinets or (if electronic) on a secure information system.

Providers may (but are not required to) make paper copies of electronic Records, provided that both paper and electronic Records are stored securely.

5.2 Electronic Record Storage Requirements

Providers that choose to store records electronically must ensure that all electronic Record storage systems operate in accordance with the storage and physical access requirements outlined in this RMI and the department's Security Policies.

Where Providers migrate electronic Records to a new storage device or system, or change the file format of an electronic Record, Providers must comply with GRA-31 in destroying the source record (i.e. the original electronic Record). Refer to *Section 3: Agreement Records* for more information on GRA-31.

Providers that choose to outsource the storage of electronic records to a third party should be aware that the requirements outlined in this RMI, the department's Security Policies, the Agreement or any relevant policy or legislation for the storage of electronic records, applies to third party hosting arrangements. This includes all relevant privacy, security and system requirements.

Providers must not transfer electronic Records to, or store electronic Records with, third party data hosting entities, including cloud storage providers, without the prior written approval of the department. Where the department does give such prior written approval, the Provider must comply, and must ensure that the third party data hosting entity complies, with any conditions specified by the department in providing that approval.

General advice on the management and storage of electronic records is available on the National Archive of Australia website.

5.3 Reporting Unauthorised Access, Damaged, Destroyed, Lost or Stolen Records

Providers must report all incidents involving unauthorised access, damaged, destroyed, lost or stolen Records to the department as follows:

- notify your Relationship Manager using *Attachment A: Provider Incident Report* no later than the Business Day after the incident.
- report any incidents involving stolen Records to the police immediately.
- make every effort to recover lost or damaged Records (e.g. retrieving or photocopying Records) wherever possible.
  Note: damaged Records must not be destroyed without authorisation from the department.
- if required, arrange and pay for the services of expert contractors (e.g. disaster recovery or professional drying services).
- prepare a detailed report of the incident, including details as appropriate to the incident (e.g. condition of Records – which could include photographs, recovery plans, proposed retrieval action, details of any potential breaches of privacy obligations etc.).
- forward this detailed report to your Relationship Manager as soon as possible and in any case within 15 business days of the incident.
- inform Participants if any Personal Information has been lost or is at risk of being publicly available.
- if necessary, reinterview Participants to recollect information.
- review Record storage standards and access protocols to ensure their adequacy in future. The department may make recommendations to the Provider to mitigate the risk of re-occurrence of the incident.

6. Control of Records

Providers must be able to locate and retrieve Records about a Participant if requested.

Providers must inform their Relationship Manager if they become party to legal action so that arrangements for the appropriate retention of Records can be organised.

6.1 Records List

Providers must maintain an up to date list of the Records held by the Provider and make this list available to the department upon request. This list should contain sufficient information to clearly identify the content and location of a Record in a search process. The list must be created and managed in an electronic format (ideally Microsoft Excel or equivalent or a comma or tab delimited format) that the department can read.

Providers may wish to identify on the Records list whether Records are:

- Priority – pertaining to current or future legal action (refer below)
- 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 – Records have been returned to the department

Examples of Priority Records (also referred to in *Attachment C: Records Retention Periods*) are where the Provider may be aware of the following:

- a complaint
- an injury caused by or to a Participant
- a possible claim for compensation
- current or pending legal action

Refer to *Section 8: Records Retention* for information on the retention of the Records list.

7. Transfer of Records

7.1 Transfers between Providers

Clause 44.7 of the Agreement provides that, subject to clause 41 [Personal and Protected Information] and clause 62 [Transition Out], Providers must:

(a) not transfer, or be a party to an arrangement for the transfer of custody of the Records to any person, entity or organisation other than to the department, without the department's written approval and;

(b) where transferring Records, only transfer the Records in accordance with these Guidelines or as otherwise directed by the department.

Records must only be transferred between Providers if this is required to continue providing Services to Participants. In such cases, Records must be transferred securely by Providers and as soon as possible and in any case within 28 Business Days of a request to transfer Records. A list of all Records (as per *Section 6.1: Control of Records – Records List*, above) being transferred should be provided to the receiving Provider.

Where the transfer of Records containing Personal Information and Protected Information is permitted under the *Privacy Act 1988* (Cth) and the *Social Security (Administration) Act 1999* respectively, written approval from the department is not required.

When a Provider is transferring Records off-site to another Provider, for storage, secure destruction or to the department, it remains the Provider's responsibility to ensure information is secure during the transfer process.

7.2 Transfer of Personal Information outside Australia

Providers must not transfer Personal Information outside Australia, or allow parties outside Australia to have access to it, without the prior written approval of the department.

8. Records Retention

Providers must retain Records according to the minimum retention periods outlined in *Attachment C: Records Retention Periods*.

Providers must review Records that have reached the minimum retention period before destroying in accordance with the RMI. If a Record has reached the required minimum retention period but, for example, the Provider has knowledge of legal action or potential legal action, the Record must be re-sentenced[1] and the Relationship Manager informed.

Retention periods apply to all formats of Records, whether created in paper or electronically or scanned.

Note: 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. For more information regarding this, please refer to *Section 3.1.2: Agreement Records – Requirements – Conditions*.

Refer to *Section 10: Destruction of Records* for more information on destroying Records.

9. Return of Records

Records must be returned to the department within 28 Business Days if requested by the department.

Providers must obtain the department's approval prior to returning any Records to the department as the return of records will be reviewed on a case-by-case basis as Providers are required to have records management provisions as per the Agreement and as outlined in these Guidelines. Providers may seek permission to return Records to the department following the Completion Date and should do so by completing *Attachment B: Provider Request to Return Records* and submitting to their Relationship Manager who will verify if records can be returned to the department. Please note that the request must be accompanied by a list of the Records the Provider is requesting to return.
The following is provided as a guide when returning records to the department (either requested by the department or via approval to return):

1. Completion of Attachment B by the Provider outlining reason for return and particulars of the request;
2. Provider ascertains how many cartons are required to complete the safe retrieval of records;
3. Relationship Manager to notify Information and Records Management Team of the request and forward request details;
4. Approved requests: Provider will be sent cartons and barcode labels from the Information and Records Management Team;
5. Provider to fill cartons and complete spreadsheet detailing contents of files and file particulars (as per 7.1 Records List);
6. Relationship Manager verifies spreadsheet list and approves pickup of files;
7. Spreadsheet is sent to Information and Records Management Team to update departmental system;

[1] NAA definition: The process for identifying the disposal class a record belongs to and applying the disposal action specified in the relevant disposal authority. Sentencing is the implementation of decisions made during appraisal.

8. Iron Mountain/Courier organise to collect cartons via Relationship Manager – Relationship Manager to notify Provider of pick up details; and
9. Information and Records Management Team notified of collection and update system or relevant storage location.

Refer to *Section 6.1: Control of Records – Records List* for information on list requirements.

Providers with a continuing contractual relationship with the department will be required to manage Records of Participants who have ceased receiving Services in accordance with the previous contractual arrangements in effect at that time (e.g. ESC3 RMI). Records of Participants continuing to receive Services are required to be managed in accordance with the Agreement and the RMI.

9.1 Electronic Records

Providers creating electronic Records should consider using a format that will allow the department to read Records if returned to the department in future. The department requests that electronic Records be created and managed in Microsoft Office (or the open source equivalent) formats, or in PDF format. The department will advise Providers if departmental system requirements change significantly during the Term of the Agreement.

Electronic Records contained in the department's IT system (the Employment Services System [ESS]) do not need to be returned.

9.2 Access to Returned Records

Where Records have been returned to the department and a Provider requires access, the Provider must write to their Relationship Manager with the details and purpose of the request. The department will consider these requests, but may require Providers to seek access via the freedom of information process as required under the *Freedom of Information Act 1982*.

Where Records have been returned to the department and a Provider receives an order to produce documents contained in the Records, such as a subpoena, the Provider should seek independent legal advice.

10. Destruction of Records

Providers must not destroy or dispose of Records other than in accordance with the RMI or as directed by the department. When Providers destroy Records, they must use a method that ensures information is no longer readable and that it cannot be retrieved.

Subject to *Section 3: Agreement Records*, Providers must only destroy Records that have reached the minimum retention period and following a review process as outlined in *Section 8: Records Retention*.

Records must not be destroyed where Providers are aware of current or potential legal action, even if the minimum retention period is reached. These Records are Priority Records, and must be retained in accordance with requirements set out for Priority Records in *Attachment C: Records Retention Periods*. A Provider must also comply with any direction from the department not to destroy Records.

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 *Section 6: Control of Records* for more information on the tracking of Records and *Section 8: Records Retention* for more information on retention periods.

10.1 Methods of Destroying Paper-Based Records

Commonwealth policy requires that paper-based Records must only be destroyed using one of the following methods:

- ***Pulping*** – transforming used paper into a moist, slightly cohering mass, from which new paper products will be made;
- ***Burning*** – in accordance with relevant environmental protection restrictions;
- ***Pulverisation*** – using hammermills with rotation steel hammers to pulverise the material;
- ***Disintegration*** – using blades to cut and gradually reduce the waste particle to a given size determined by a removable screen; and
- ***Shredding*** – using crosscut shredders (using either A or B class shredders).

If destruction of paper 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.

10.2 Methods of Destroying Electronic Records

It is a Provider's responsibility to ensure that all electronic Records are identified and removed from systems and destroyed.

Electronic Records can only be destroyed using one of the following methods:

- digital file shredding;
- degaussing (i.e. the process of demagnetising magnetic media to erase recorded data); and
- physical destruction of storage media (e.g. pulverisation, incineration or shredding).

Re-formatting may also be used as a method of destroying electronic Records if it can be guaranteed that the process cannot be reversed.

Provider Incident Report

Australian Government
Department of Social Services

Disability Employment Services

Use this form to report to the Department of Social Services (the Department) data incidents that involve personal information and records held by a Provider.

Privacy incidents may involve any unauthorised access, disclosure or loss of personal information, including damaged, destroyed or stolen records.

This form is in two parts, (1) initial incident reporting and (2) detailed reporting, and is designed to be progressively updated and submitted, as details of the incident become known over the investigation, assessment and notification processes.

- **Part 1** must be completed and submitted to the Department *no later* than **one business day** after the date of a privacy incident or (if different) when the incident is first discovered.

- **Part 2** must be completed and submitted to the Department within **15 business days** of the privacy incident (and earlier wherever possible).

The form may also be used by Providers to undertake mandatory reporting of 'eligible data breaches' to the Office of the Australian Information Commissioner (OAIC), in accordance the Notifiable Data Breaches (NDB) Scheme. It is recommended that you read the resources provided by the OAIC about the NDB Scheme and guidance on reporting a data breach.

Part 1 - Initial Reporting

Part 1A – Provider Information	
Provider Name	
Provider Org Code	
Site Name and Site Code	
Name of person completing report	
Position	
Phone / Email	
Date of submission to the Department	
Part 1B – Details of the Incident	
Date of privacy incident (if different, the date when incident was first detected)	
Provide a description of the incident. Include what operational systems were or may be affected and how the unauthorised access, loss or theft occurred. If relevant, why were the Records vulnerable?	
How was the incident discovered?	
What type of information was involved in the incident? (e.g. financial details, TFN, identity information, contact information, health or other sensitive information).	
Has anyone (or is anyone likely to have) obtained access to the information?	
Was the incident considered deliberate or inadvertent?	
Was anyone else notified or a witness to the incident? If yes, provide details.	
Has the incident been assessed in accordance with the NDB Scheme and is it considered an '*eligible data breach'*? Please explain why/why not and provide reasons.	*<u>Note:</u> if the answer is unknown at the time of submitting this report, state this. Part 1 is due no later than one Business Day after the date of the privacy incident.*

Part 1C – Affected parties	
Whom does the data breach affect? (E.g. job seekers, participants, general public, other government agencies, any other third party).	
Provide the exact number of individuals affected (if known). If not known, please provide your best estimate.	
Do you have current contact details for affected individuals?	
Part 1D – Initial Action	
Describe the immediate remediation/containment actions taken (e.g. retrieval of records).	
Have affected individuals and/or the Australian Information Commissioner been notified of the incident and when?	
Was anyone else notified of the data breach? (E.g. police, security consultant or support team, etc.) Provide contact details and when.	
(If applicable) Based on initial remedial action(s) taken, is this breach still considered a potential 'eligible data breach' under the Notifiable Data Breaches (NDB) scheme? Why?	*NB: if your remedial action is successful in making serious harm no longer likely, then the notifications to the OAIC and affected individuals is not required under the NDB scheme.*
If applicable, please provide the following: ▪ Photos of damaged Records ▪ A list of damaged/lost/stolen Records ▪ Copies or a list of documents relevant to the incident	

Part 2 – Detailed Reporting

Note: *Depending on the nature of the privacy breach or incident, not all questions/sections may be relevant. Please note 'N/A' accordingly. If details previously provided in Part 1 remain accurate and fulsome, feel free to refer to those relevant sections in completing Part 2.*

Part 2A – Investigation	
Describe the investigation undertaken and the evidence and findings. (Evidence of the breach and remedial action must be preserved)	
Part 2B – Rectification/Remediation Action	
Describe the actions taken to address the privacy incident and prevent harm to affected parties. (E.g. retrieval of records etc.)	
Have steps been taken to prevent the breach from occurring again?	
Is there any other further action proposed?	
Part 2C – Eligible Data Breach	
Has the incident been assessed in accordance with the NDB Scheme and is it considered an 'eligible data breach'?	
Have affected individuals and the Office of the Australian Information Commissioner been notified of the breach and when? (Please describe how affected individuals will be or were informed about the breach of their personal information).	
If you do not intend to notify individuals because of an exception, please provide your reasons, including details about a relevant exception under the *Privacy Act 1988*.	

Additional Information? (Please include any relevant information that you believe is important)

****If applicable, please provide a statutory declaration for Part 2**, stating the Records are damaged beyond salvage or were lost or stolen.

I confirm the details and attachments provided in this final version of the report (Parts 1 and 2) are accurate and correct and the CEO (or equivalent) <insert CEO's name here> has been informed of this data breach.

Name: _____ Title: _____

Date:

Provider request to return Records

Australian Government
Department of Social Services

Providers must complete this form before Records are returned to the Department of Social Services (DSS). Return of files to the department are approved on a case-by-case basis and Providers should have their own provisions for Records Management.

- Provider to complete Section 1 and submit to their Relationship Manager (RM).
- RM to complete Section 2 and forward to DSS' Information and Records Management Team.
- Provider to liaise with RM in relation to the progress of their request.

Section 1 – Provider to complete	
Provider legal name and ABN:	Contact person:
Provider address:	Phone number:
Total number of cartons expected:	Service(s):
Expected retention:	Time left on retention:
Contents spreadsheet completed: Yes/No (please select)	
Reason for request to return:	
Section 2 – Relationship Manager to complete	
Name and phone number:	Signature / /
Reason for return of Records:	
Section 2 – Information and Records Management Team to authorise	
Name of IRMT Officer:	Signature / /
Final action:	

A list of all Records the Provider is requesting to return must be attached to this pro forma, and must contain information as specified in *Section 6.1: Control of Records – Records List*.

Records Retention Periods

Records Authority (RA)

The Employment Services Records Authority 2009/00179260 (RA) issued by the National Archives of Australia (NAA), groups together categories of Records with the same minimum retention periods and uses broad terms to assist with the sentencing of Records. The RA gives the legislative framework for the destruction of Records following retention periods as set out in the RMI.

The Records description and examples below help Providers to identify appropriate retention periods based on the type of Record. The numbers included under the 'Entry' heading in each table are the classification numbers from the RA and the term 'last action' is defined as the 'last action taken or the last recorded information' relating to that Record.

The overarching introduction to classifications in the Employment Services RA states:

"The function of implementing labour market programs. Includes managing and coordinating the delivery of employment services and assistance to job seekers; administering the provision of grants and programs to assist targeted groups in the community, such as Indigenous Australians and disadvantaged job seekers; and liaising with local communities."

Note: Providers have the discretion to retain Records longer than the minimum periods outlined below, but must not reduce any retention periods. In addition, the department may direct that some Records be retained for longer periods, for example, in the case of Records required in any legal action.

RA interpretation

Priority Records

Priority Records are specified in Table 1 below. All Priority Records require the utmost attention of Providers to ensure access as required by the department. In addition to the retention policy below, where there is potential for any legal action, Records must be retained until the matter is resolved.

Table 1: Priority Records

Entry	Description of Records	Includes but is not limited to	Disposal action
20184	Records documenting accidents or incidents to participants engaged in employment services programs, including all relevant records associated with that participant.	▪ Incident / accident information ▪ Potential legal action / fraud Records ▪ Customer Feedback Register ▪ Risk assessments ▪ Other related documentation	Destroy 6 years after last action unless legal action or litigation is underway, in which case the Records must be retained after 6 years until the matter is resolved
20185	Register of complaints about pre-employment and employment services, including any and associated documentation.		
20192	Records documenting the services provided to participants engaged in community, voluntary and work experience projects.		

General Services Records

This category encompasses Records involving the provision of employment Services to Participants. However, if there is any indication that a Record may be required in relation to legal action, the Record must be re-categorised as a Priority Record and managed accordingly.

Table 2: General Services Records

Entry	Description of Records	Includes but is not limited to	Disposal action
20186	Records documenting the processing of project business proposals from participants for assistance under self-employment program schemes, including the assessment of applications, the monitoring and mentoring of participants and records documenting the payment of fees to the providers of these services.	▪ Employment Pathway Plans ▪ Activity agreements ▪ Proposed NEIS business plans ▪ Monitoring / mentoring information ▪ Non-work experience placement / service ▪ Services and support provided to the Participant ▪ Criminal records checks and other background checks ▪ Other related documentation	Destroy 3 years after last action
20195	Records documenting the successful proposals for all Work Experience activities. Includes receipt, assessment and notification to applicants, project work plans, proposals, outcomes, milestones, performance indicators and successful requests for review of a decision.		
20199	Records documenting the provision of employment services, other than work experience or limited services.		