s22

Australian Government

Services Australia

Restricted Access and eligibility 104-06000000

Currently published version valid from 1/05/2025 7:13 PM

Background

s22

This document outlines information about Restricted Access and its application for protection of customer information and the roles of Restricted Access Service Officers. Restricted Access for Centrelink customers was formerly known as the Deny Access Facility (DAF).

Government intent

Restricted Access is available for Centrelink customers seeking additional protection of personal information held by Services Australia. It is a computer based security system, which denies access to the customer's Centrelink computer record for the majority of staff. Only a limited number of the agency’s staff can access the record. Temporary access may also be authorised for specialist staff. The purpose of Restricted Access is to protect the customer's location details. Restricted Access is not a tailored service arrangement for customers to choose who can service them.

Restricted Access is available to customers:

- who have genuine fears for their safety
- have a Security Notice Issued (SNI) by the Attorney General applied
- where there is a risk that a staff member could endanger the customer by accessing the customer's computer record
- in exceptional circumstances where the customer's record required a higher level of protection

Restricted Access should only be used in exceptional circumstances.

Determining eligibility

Customers may be considered eligible for Restricted Access because of, but not limited to, the following reasons:

s47E(d)

Restricted Access is also applied to records of customers whose welfare payments have been cancelled - Security Notice Issued.

In these cases:

- customers subjected to a Security Notice must not be provided with contact details of the responsible Restricted Access Officer

- records subject to a Security Notice will be 'Restricted Access' to minimise application or re-application for payment. These records are managed by a central processing team within Business Integrity Division

See also Witness Protection Information and Centrelink customer requests a new Customer Reference Number (CRN).

Discuss alternate options

As Restricted Access limits the customer's access arrangements with the agency, it should only be used in the most serious cases. Intermediate security measures, such as passwords, should be considered as a more user friendly option.

Customers engaged in Family Court matters should be made aware that Restricted Access will not prevent the agency from disclosing their location to the Family Court when ordered to do so.

Level of protection

Restricted Access only offers protection to a person's electronic Centrelink record. Their paper file, if one exists, remains in Records Management Unit (RMU). It is important that customers seeking protection are made aware of this. Restricted Access does not replace other forms of protection which are in place for all customers. It is the highest level of protection the agency offers to customers assessed as requiring protection above that offered by the 100% logging process and other security measures.

If the customer who is granted Restricted Access is partnered, both records must have Restricted Access applied, as the customer's information may be accessible through the partner's record. If Restricted Access is not applied to both members of a couple, the link between the records may cause problems when accessing the records. Other customers, who reside with the Restricted Access customer, may need to have Restricted Access applied to protect the customer's whereabouts. All customers who have Restricted Access applied must be notified of their servicing arrangement.

Staff with access to Restricted Access records

Only staff holding specific skill tags and security role can access a Restricted Access record.

All Restricted Access customer records are assigned an ORG unit. The National Restricted Access Team (NRAT) or Restricted Access Business Administrators control access to the record. Temporary access for up to 7 days can be provided to other staff for completion of specific tasks. Access by Irregular and Intermittent (IIE) and Contractor staff to Restricted Access records is granted only in exceptional circumstances when non-IIE/Contractor staff are not available.

Access by non-Restricted Access staff for specific tasks

Staff may require access to a Restricted Access record for a specific task, including (but not limited to):

- specialist work
- ICT investigations, and
- processing work allocated through Workload Manager

If staff without access to the Restricted Access record attempt to enter the record, a warning displays advising that access to the record is restricted.

Temporary Access

The NRAT or Restricted Access Manager may approve temporary access for a period of up to 7 days. Each Restricted Access customer can have a maximum of one Temporary Officer at any time.

To be granted temporary access to a Restricted Access customer record, staff must:

- be an ongoing employee at the APS3 level or above
- have a business need to access record
- have the required security roles and skill tags. **Note:** staff can apply for these but it can take up to 24 hours for them to be applied

To make a request for temporary access, refer to the National Restricted Access page.

Role of Service Officers

Restricted Access customers receive telephone service from authorised Restricted Access Officers in the National Restricted telephony queue. Some customers elect to receive face-to-face service by a dedicated Restricted Access Manager in their Service Centre.

All agency staff are responsible for processing activities allocated to them, which relate to Restricted Access customers. Temporary access can be granted where required.

If any activity is selected for Quality On Line (QOL)/Quality Management Application (QMA), checkers will require Temporary Access to complete.

Role of National Restricted Access Team and Restricted Access Business Administrator

The National Restricted Access Team and Restricted Access Business Administrators have overall responsibility for administering Restricted Access, including the following:

- Deciding whether a customer should be granted Restricted Access
- Applying Restricted Access on the customer's record and, if applicable, the partner's record; and/or family member's records
- Discussing self service options including:
    - Centrelink online services
    - letters online (Centrelink Online Letters or myGov Inbox)
    - Electronic Messaging, and
    - phone self service
- Ensuring the Access Officer positions are covered during absences
- Arranging temporary access for other staff who require access to the customer's records
- Conducting annual reviews of Restricted Access customers to assess if there is a continuing need for Restricted Access
- Maintaining the Restricted Access Relationships tab by adding or removing access for Restricted Access managers, officers or temporary officers
- Handling urgent enquiries about Restricted Access
- Reporting problems experienced with Restricted Access to the Privacy Section
- Handling enquiries, suggestions for change or complaints about Restricted Access
- Providing policy advice to the network about Restricted Access

Contact details for individual staff in the National Restricted Access Team **are not** to be given to customers or external agencies.

The Resources page contains links to the:

- Skill Tag and Access Request
- request for temporary access to a Restricted Access record form, and
- contact details for the National Restricted Access Team

Contents

Administration of Restricted Access

Support, maintenance and FAQs for Restricted Access

Related links

Privacy, sharing and storage of customer information

Centrelink customer requests a new Customer Reference Number (CRN)

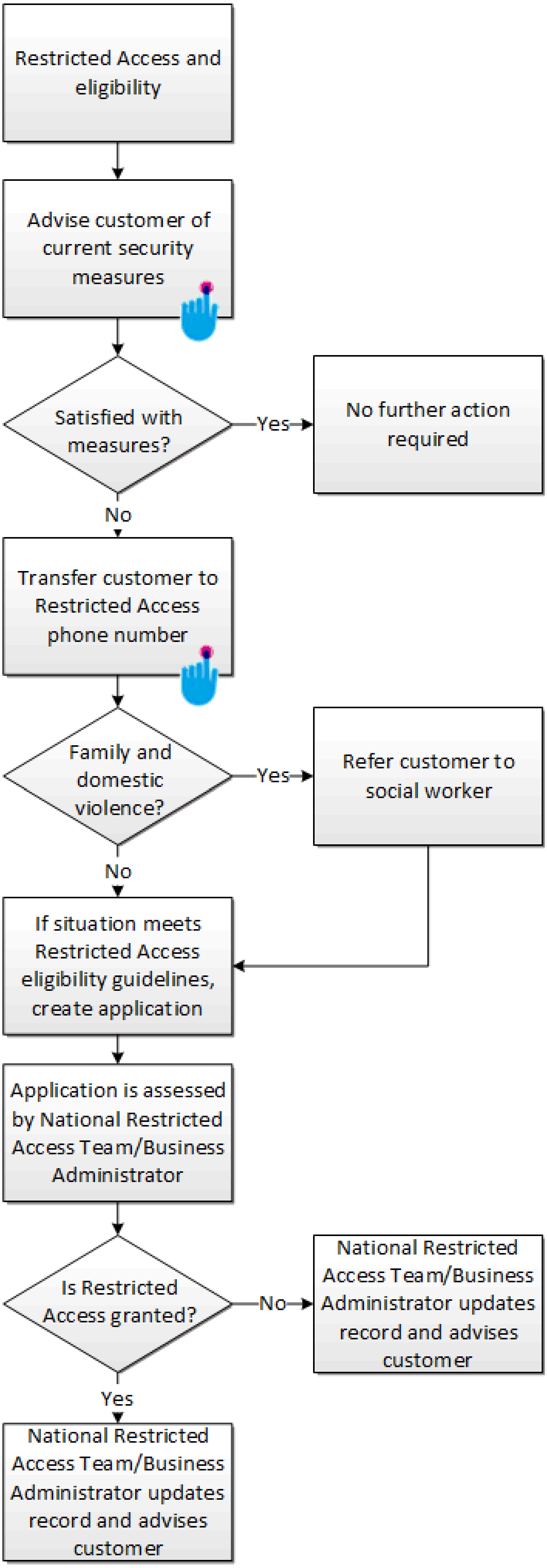
Process Summary

Flowchart

Assessing eligibility for Restricted Access

This image provides a summary of the process to assess a customer’s eligibility for Restricted Access.

Note: a text based version of the following process summary image is available.


Restricted Access and eligibility
Advise customer of current security measures
Satisfied with measures?
Yes
No further action required
No
Transfer customer to Restricted Access phone number
Family and domestic violence?
Yes
Refer customer to social worker
No
If situation meets Restricted Access eligibility guidelines, create application
Application is assessed by National Restricted Access Team/Business Administrator
Is Restricted Access granted?
No
National Restricted Access Team/Business Administrator updates record and advises customer
Yes
National Restricted Access Team/Business Administrator updates record and advises customer

Process

This page contains the process for initial assessment by Service Officers and processes for the National Restricted Access Team.

On this page:

Service arrangement for customers with Restricted Access in place

Assessment of a customer's eligibility for Restricted Access by Service Officers

Service arrangement for customers with Restricted Access in place

Table 1

Step	Action
1	**Is Restricted Access in place** + Read more ... If a customer has Restricted Access in place, when their record is accessed in: - Process Direct a Sensitive data warning message will display - Customer First the s47E(d) screen will display Does the customer have Restricted Access in place? - **Yes**, go to Step 2 - **No**, and they are concerned with security of their personal information or safety, see Table 2
2	**Customer has Restricted Access** + Read more ... Channel the customer contacted: - Phone call, go to Step 3 - Service Centre, go to Step 4 - Process work item allocated in Workload Manager (WLM), go to Step 5
3	**Customer contacts by phone call** + Read more ... Restricted Access customers are serviced through the Restricted Access telephony queue. Remind the customer to contact using the Restricted Access phone number. **Cold transfer** the customer using the s47E(d) s47E(d) option to complete their business. If sensitivities are identified a warm transfer may be deemed more appropriate. Procedure ends here.
4	**Customer contacts face-to-face** + Read more ... Does the Service Centre manage the customer's Restricted Access? - **Yes**, proceed with servicing the customer as per Restricted Access arrangement. Procedure ends here - **No:** ○ Direct the customer to contact using the Restricted Access phone number ○ Immediate temporary access can be granted to Process Direct if needed to complete customer business ○ Contact the National Restricted Access Team through their positional mailbox ○ Procedure ends here
5	**Processing Work Item** + Read more ... **Accessing the customer's record in Customer First/Customer Record**

	• Apply these skill tags in s47E(d) ○ s47E(d) ○ ○ See Resources page for a link to the Skills Tag and Access Request page to follow for temporary access to be granted to a Restricted Access record • Complete the Request for temporary access to a Restricted Access record form. See Resources page for link to the form **Accessing the customer's record in Process Direct only** Complete the Request for temporary access to a Restricted Access record form. See Resources page for link to the form. When access has been granted, the work can be processed. **Only** reassign or re categorise work items if one of the relevant unassign/reassign reasons is met. **Staff and leaders** Email National Restricted Access Team for: • advice on requesting temporary access, or • any other enquiry for a Restricted Access customer Procedure ends here.

Assessment of a customer's eligibility for Restricted Access by Service Officers

Table 2

Step	Action
1	**Customer concerned with security of their personal information or safety** + Read more ... Advise the customer of current measures in place, including 100% logging of staff access. **Discuss alternate options** As Restricted Access limits the customer's access arrangements with the agency, it should only be used in the most serious cases. Intermediate security measures, such as passwords, should be considered as a more user-friendly option. Customers engaged in Family Court matters should be made aware that Restricted Access will not prevent the agency from disclosing their location to the Family Court when ordered to do so. The Resources page has a link to the Services Australia website for further information for customers. Is the customer satisfied with these security arrangements? • **Yes**, procedure ends here • **No**, go to Step 2
2	**Refer customer to the National Restricted Access Team** + Read more ... If a customer requests further security for their Centrelink customer record, service centre and Smart Centre officers must **warm transfer** the customer to s47E(d) using the s47E(d) . For more information, see the National Restricted Access Intranet page. Was the warm transfer successful? • **Yes:** ○ Service delivery officers, procedure ends here ○ National Restricted Access Team, go to Step 3 • **No:** ○ See the National Restricted Access Intranet page to complete a referral for Restricted Access ○ Service delivery officers, procedure ends here

3	**Explain Restricted Access to the customer - National Restricted Access Team (NRAT)** + Read more ... Examine all possible alternatives before suggesting Restricted Access. It may be necessary for a social worker to discuss the customer's concerns with them during the interview and assessment process. If the customer is in crisis or experiencing family and domestic violence, it may be appropriate to refer customers to a social worker. Explain the limitations that Restricted Access will impose on the customer’s dealings with Services Australia and the limited security that Restricted Access provides. For example: • Explain that Restricted Access only limits staff access to their Centrelink computer record • If the customer is partnered, **both records** must have Restricted Access applied, as the customer's information is accessible through the partner's record. If Restricted Access is not applied to both records, the link between the records will cause access issues • Other Centrelink customers, who **reside with the protected customer**, may need to have Restricted Access applied to their record to protect the customer's whereabouts • The customer must provide a postal address if Restricted Access is granted • Customer may elect to **unsubscribe** from self service including: ◦ Centrelink online services ◦ letters online (Centrelink Online Letters or myGov Inbox) ◦ Electronic Messaging ◦ phone self service • Services Australia exchanges information with other Government agencies. Advise the customer they should notify other Government agencies they deal with, that they would like their personal information kept secure. Explain that other agencies may not have similar security measures in place Does the customer wish to have Restricted Access applied? • **Yes**, complete a referral to the NRAT mailbox. Procedure ends here • **No**, confirm the customer understands the other security measures available. Procedure ends here

Resources

Intranet links

National Restricted Access

Skill Tag and Access Request

Forms

Request for temporary access to a Restricted Access record form

Contact details

National Restricted Access Team

s22

Australian Government

Services Australia

Restricted Access Customer System (RACS) 104-20102324

Currently published version valid from 23/06/2025 3:04 PM

Background

s22

This document outlines the administration process for RACS in child support. It explains:

- the RACS status of customers
- the role of RACS coordination, and
- how staff can apply for RACS access

Service delivery model for RACS customers

The National RACS Team is located in Brisbane. This team manages the majority of RACS customer's needs. Additional RACS officers are located in:

- Adelaide to support Brisbane and manage staff conflict customers
- various locations to provide New Customer and other specialised functions

Categories of Restricted Access Customers

There are 3 categories of customers maintained in RACS.

Customers at Personal Risk

Includes people who may suffer harm if their personal details, especially their home address or place of employment is disclosed.

An objective assessment of the customer's circumstances is carried out to decide if RACS status is needed. Points to consider, include, but not limited to:

s47E(d)

Staff as customers

Staff as customers includes people who have a customer association to Child Support:

- Employees and their partners
- Contractors, their employees or subcontractors with access to Child Support computer or hardcopy systems containing case details
- Customers who have a representative who is a Child Support employee

- Employees of government agencies who have access to Child Support computers or hardcopy systems containing case details
- Service providers who have access to Services Australia computer or hardcopy systems, containing Child Support case details

Services Australia staff who are customers are not always made RACS customers unless they:

- work directly to Child Support, and
- have access to child support computers or hardcopy systems containing child support customer details

All staff have a responsibility to remain alert to real and perceived conflicts of interest and escalate any matters via email to RACS Coordination.

Staff members who are also a customer or representative need to call Child Support, the same as customers who do not work for Child Support. They must not directly approach a Service Officer about the case. Direct contact may compromise the integrity of the:

- Child Support Scheme
- Service Officer approached, and
- Customer or staff member

RACS officers must make sure they give the same service to customers or customer representatives who are also staff as they would to any other customer.

Special Interest Customers

Include, but not limited to customers:

s47E(d)

Staff disclosure statement

Regardless of if staff in Child Support are a customer they must complete the RACS Disclosure Statement form:

- on engagement
- if their personal circumstances change after engagement. For example they become a:
  - Child Support customer
  - customer representative, or
  - enter a domestic partnership with a customer
- at the request of a RACS Coordinator or manager
- when requesting access to RACS

Roles and Responsibilities

RACS Coordinator

- Administers and oversees RACS to make sure that it meets the Protective Security Policy Framework (PSPF) minimum standards for information security
- Approve access to s47E(d) – ability to access, add, remove or change customer RACS
- Approve access to add RACS to both human and non-human position in Cuba
- Assess and action RACS disclosure forms, store securely as per the Protective Security policy Framework (PSPF)
- Assign, review, change and remove RACS levels of customers
- Coordinate and authorise access to RACS level 1, 2 and 3. Ensuring that staff accessing hold the necessary security clearances
- Oversee and monitor Cuba based RACS reports to identify and manage the numbers of RACS customers and the number staff with RACS access
- Provide advice on customers RACS requirements
- Provide advice on granting RACS access
- Support staff to use child support RACS procedures. Make sure staff are aware of their responsibilities through induction programs and ongoing training

Work with and support other RACS Coordinators to apply the child support RACS policy principles consistently

Human resources/recruitment

- Put the 'RACS disclosure forms' in the recruitment pack issued to new staff

Team Leader of RACS officers

- Oversee and monitor the number of staff in their team with RACS access
- Make sure that staff leaving their team have their RACS access removed
- Make sure that all paper based RACS records are labelled, stored and disposed of appropriately
- Make sure that staff report and document 'conflict of interest' situations

Service Officers with RACS Access

- Under go regular privacy and security awareness training
- Declare and manage any conflict of interest via the RACS disclosure and Inadvertent Access forms
- Access information in line with the need to know principle
- Tell the team leader/RACS Coordinator when RACS access is no longer needed
- Consider the RACS status of a customer when processing information. Tell the RACS Coordinator if a review is needed

Service Officers

- Undergo regular privacy and security awareness training
- Declare and manage any conflict of interest via the RACS disclosure and Inadvertent Access forms
- Access customer record in line with the need-to-know principle

Team leaders

- Make sure staff understand their obligation to disclose conflicts of interest
- Proactively seek the removal of RACS access in Cuba for staff members when it is no longer needed

OP PLAN REALTIME

- Complete the processing for staff to have access to RACS and maintains records of approved accesses

Staff Facing Products – Cuba and Pluto

- Provide s47E(d) access and review accesses due to expire in consultation with RACS Coordination, to contact see Child Support - national and site mailboxes > Staff Facing Product

Related links

Australian Taxation Officer (ATO) and the Services Australia Information Hub

Inadvertent access and authorised access

Witness Protection information

Customer records Cuba Process Help

RACS Details Window Help

Process

This document outlines the administration process for RACS in child support. It explains:

- the RACS status of customers
- the role of RACS coordination, and
- how staff can apply for RACS access

On this page:

Staff disclosure

Potential RACS and review RACS classification

Apply for RACS officer access

RACS customers on the ATO system

RACS customers and online services

Staff disclosure

Table 1

Step	Action
1	**Staff disclosure statement** + Read more ... All child support staff must complete the RACS Disclosure Statement if they are a: • Child Support customer • customer representative • partner of a Child Support customer, or • close friend or relation to a Child Support customer Staff complete the form: • on engagement • if their personal circumstances change after engagement. Such as they become a child support customer, a customer representative or enter into a domestic relationship with a child support customer • at the request of a RACS Coordinator or manager • when requesting access to RACS This will make sure that: • staff are not processing information of a colleague they know personally • staff who are customers, or customer representatives, have their Child Support matters dealt with privately and not by colleagues in the same state • customers who know that the other customer in the case is a Child Support staff member will be assured that the staff member is not being treated favourably • the Privacy Commissioner, is satisfied safeguards are in place to prevent staff processing information of colleagues they know personally
2	**Complete the RACS Disclosure Statement form** + Read more ... Staff complete the RACS Disclosure Form online and select 'Submit'. Procedure ends here for Service Officers.
3	**Assessment of RACS Disclosure Statement form** + Read more ... RACS Coordinators assess the disclosure statement to determine if a conflict of interest exists and if a restriction is needed. Is there case information to be restricted? • **Yes**, RACS Coordinator will: ○ Determine the appropriate RACS security level and update the Cuba record ○ Transfer the case out of the state where the staff member works ○ Review all case information to make sure it is correctly restricted at the appropriate level • **No**, RACS Coordinator will: ○ file the disclosure statement **Note:** if the RACS Coordinator needs more information to make a decision, they will contact the service officer.

Potential RACS and review RACS classification

Table 2

Step	Action
1	**Possible RACS customer identified (Service Officer)** + Read more ... Email s47E(d) if a potential RACS customer is identified. Continue to manage the customer while the RACS Coordinator is assessing and making the RACS decision. Notify the RACS Coordinator if: • there is a personal relationship with the customer, such as actual conflict of interest, and/or • the customer is a staff member and is currently being managed in the same state they reside in Procedure ends here for Service Officers.
2	**Customer asks for RACS status review (Service Officer, RACS Officer)** + Read more ... Email s47E(d) if a customer asks for their RACS status to be reviewed or ended. Procedure ends here for Service Officers and RACS Officers.
3	**Review customer RACS classification (RACS Coordinator)** + Read more ... All customer RACS classification is reviewed at least every two years. A RACS review intray auto generates based on the review date set in the RACS Details window. The RACS review intray is actioned by a RACS Coordinator. Common reasons to review a customer's RACS level: • Customer is no longer employed by Services Australia or working in Child Support • Customer's partner is no longer employed by Services Australia or working in Child Support • Customer's profile has reduced
4	**Assess the customers circumstances (RACS Coordinator)** + Read more ... The level of restriction applied to an individual customer must be reflective of the level of risk to the customer or agency. Do not base the level on the reason for the restriction or the negative impact a RACS indicator may have on customer service and potentially, customer satisfaction. Use discretion when determining the customer's RACS level. Assess each situation on its own merits after considering all information. s47E(d) **Note:** the RACS status of all other parties to the primary RACS customer will automatically update. Make sure all associated customer's circumstances are considered. They may warrant a RACS status in their own right rather than just by association.
5	**RACS Decision (RACS Coordinator)** + Read more ... When adding, changing or removing RACS, the RACS Coordinator will: • make a decision based on the available information • apply a RACS category to the customer's profile • document the reason for the decision in the RACS s47E(d) . If the reason is in relation to a staff member, include the service officer's name, office location and AGS (if available) If RACS is applied to the customer's profile they will arrange for the customer's enquiry to the handed over to a RACS officer to manage.
6	**Case where customer, their current partner or representative is a Child Support staff member** + Read more ...

	A RACS status must be applied, a customer cannot elect for this not to apply. The RACS Coordinator will transfer the case out of the state where the staff member lives. To make sure the case and calls remain in the new state: The RACS Coordinator: • s47E(d) • s47E(d) • conducts regular audits to make sure customers remain locked as appropriate **Note: do not** use s47E(d) The s47E(d) on the s47E(d) generates an automated intray every 6 months. This is an opportunity to review the RACS and locked status.
7	**Assign, change or remove RACS classification** + Read more ... The assigning, changing and removing of RACS classification is actioned by: **RACS 0 customers** - Cuba automatically assigns the RACS 0 level to all customers unless a higher level is assigned. RACS 0 information is known as non-RACS **RACS 1 customers** - a RACS Coordinator **RACS 2 customers** - a RACS Coordinator with RACS 2 access **RACS 3 customers** - a RACS Coordinator with RACS3 access To add a RACS classification, see Add Restricted Access Customers (RACS) table in Customer records Cuba Process Help.
8	**Cuba and RACS** + Read more ... When a RACS status is applied to a customer in Cuba they become the 'Primary RACS customer' Cuba automatically assigns 'RACS BY ASSOCIATION' to the: • other customer/s related directly to the Primary RACS customer, and • children of the case/s **Note**: due to this automatic upgrading, carefully considered decisions regarding imposing RACS on a customer. Take into consideration the negative impact of a RACS indicator on customer service and potentially, customer satisfaction.
9	**Pluto and RACS** + Read more ... s47E(d) , RACS access in Pluto is restricted to officers with RACS 3 access and to those with a genuine business need (i.e. RACS 1 and 2 officers cannot be granted access to Pluto). Requests for Pluto RACs access are made via s47E(d) , these flow to the National RACs Coordinator for authorisation. In s47E(d) the positional role required is s47E(d) .
10	**Review and quality assurance** + Read more ... Decisions made to apply, remove, or change a RACS status are quality assured through an audit program.

Apply for RACS officer access

Table 3

Step	Action
1	**RACS officer access** + Read more ... RACS access in Cuba is granted where there is a genuine business need.

	RACS coordination will consider the following when assessing a genuine business need: • Is the officer in a specialised team where the function cannot be managed by the RACS team? • Is there other RACS officers in the same team that can manage the RACs customers? Staff in Mainstream Customer Services outside of the RACS teams do not need RACs access. s47E(d) To apply for RACS 1 access, go to Step 2 To apply for RACS 2 or 3 access, go to Step 3
2	**Apply for RACS 1 access** + Read more ... • Nominated staff member completes a: ◦ RACS disclosure statement ◦ Team leader completes the RACS access form • The RACS Coordinator considers request **New customer staff who use Work Optimiser – Child Support** Check that: • RACS access has been granted, and • Cuba has been updated To access new applications in Work Optimiser, the Team Leader or Service Officer: • s47E(d) • • Is there a genuine business need? • **Yes**, RACS Coordinator makes a decision to approve the request on merit. If approved they forward to Real Time Operations Team to update the staff members access in the system • **No**, RACS Coordinator consult with business owner for an alternative
3	**Apply for RACS 2 or 3 access** + Read more ... • Nominated staff member completes a: ◦ RACS disclosure statement and ◦ Takes a PDF copy of their security clearance from ESS and emails it to s47E(d) • Team leader completes the RACS access form • A RACS Coordinator considers request Is there a genuine business need? • **Yes**, RACS Coordinator makes a decision to approve the request on merit. If approved they forward to Real Time Operations Team to update the staff members access in the system • **No**, RACS Coordinator consult with business owner for an alternative **Note:** if the staff member does not have the appropriate security clearance, the Team Leader needs to contact the s47E(d) before obtaining clearance to make sure they support the RACS access request.
4	**Emergency or temporary access to RACS information** + Read more ... There will be occasions when a Service Officer needs to be given temporary access to customer information protected by RACS, when there is no one with the appropriate access available. This may be as a result of: • a customer death • a change in customer circumstances • customer escalation

	All business line managers need to make sure they have available staff cleared and checked to undertake work task that are foreseeable. They may have a number of staff 'security clear' (BASELINE) without 'activating' their RACS status in Cuba until needed. See Security Clearance.

RACS customers on the ATO system

Table 4

Step	Action
1	**Service Officers with RATS access** + Read more ... There are a limited number of Service Officers in child support who have s47E(d) access. This access is needed to access and update details about a customer who is RACS on the ATO system. To find a Service Officer with s47E(d) access email s47E(d) . In the email include the: • customer's Tax File Number • customer's full name • information required, for example employers declarations or s47E(d) records (s47E(d) - ATO searches) • reason for the details and for what purpose the details will be used

RACS customers and online services

Table 5

Item	Action
1	**Level 3 RACS customers** + Read more ... RACS 3 customers are unable to have online access to their Child Support account.
2	**Levels 1 and 2 RACS customers** + Read more ... RACS 1 and 2 customers are entitled to access their Child Support account online. Due to system limitations, Service Officers are unable to issue linking codes or temporary passwords to RACS customers. To link Child Support online accounts for RACS customers they must answer proof of record ownership questions in the myGov online linking application. Ensure all customer details are accurate and their online account status is ACTIVE. For information on online account activation, see CSAOnline accounts Cuba Process Help. Once confirmed, direct the customer to complete the following steps: • Login to myGov • Select View and link services • Select Child support For more information, see: • Access and troubleshooting Child Support self service • CSAOnline accounts Cuba Process Help

References

Policy

Do not share this attachment externally. See Freedom of Information   Information Publication Scheme.

Protective Security Policy Framework

Resources

Contact details

Restricted Access

Child Support – national and site mailboxes > Staff Facing Products

Real Time Operations Team

Macros

RACS call back request

Forms

s22

Request for RACS access

RACS Disclosure Statement

Intranet

Inadvertent access and Authorised access

Information Security and Awareness Section

Secure storage of information

Security Clearances

Security Hub

When and when not to make a customer record RACS

Table 1: this table gives guidance to help classify RACS information. Assess each situation on its own merits considering all details.

Customer details:	Is RACS needed?	RACS level	Cuba reason and notepad details
The customer is a Child Support staff member.	Yes	RACS 1 RACS 2 may be necessary if they are nationally well known	Reason: Staff Document the staff members Name (if different to customer name in Cuba) AGS number and office location. For example, ‘Customer is staff member (name), (AGS), located in Brisbane office’
The customer’s representative is a staff member.	Yes	RACS 1	Reason: Staff conflict Document the staff members Name, AGS number

			and office location. For example, 'Customers representative is child support staff (Name), (AGS), Adelaide office'
The customer is a partner of a staff member.	Yes	RACS 1	Reason: Staff conflict Document the staff members name, AGS number and office location. For example, 'Customer is partner of staff member (Name), (AGS), (office location)
The customer is a child, parent or sibling of a staff member.	No	RACS 0	n/a
The customer is a close friend of a staff member.	No	RACS 0	n/a
The customer is a person a staff member regularly talks to. For example, neighbour, vet, doctor, newsagent.	No	RACS 0	n/a
The customer demands to be made RACS, to get special treatment.	No	n/a	The appropriate customer escalation model should be followed.
The customer does not have Child Support system access but works for: • Centrelink • Medicare **Note**: co-located Centrelink or Medicare staff with Child Support may be considered for RACS 1 on a case by case basis.	No	RACS 0	n/a

s47E(d)

RACS Policy Principles

Table 2: the RACS policy principles are applicable to all RACS information and must be incorporated into both electronic systems and hard copy processes.

Principle	Description
1	**Only customers falling within defined RACS categories are to be afforded RACS status** The integrity of RACS relies upon the number of customers afforded RACS status being confined to those who have a genuine requirement, as defined by the RACS Categories. Therefore, regular monitoring and reviewing of RACS status is important to make sure that customer records, which no longer need RACS protection have the RACS status changed to avoid unnecessary protection, service delivery delays and administrative costs.
2	**A Child Support staff member who is a Child Support customer or authorised customer representative must make sure that access to that Child Support customer record is restricted through the RACS process** The management of all child support staff cases must be transparent and objective. It is the responsibility of any child support staff member who is or becomes a Child Support customer or authorised customer representative to make sure that restricting access to that Child Support customer record is considered by completing a RACS disclosure statement.
3	**Staff who are customers or customer representatives cannot be managed in their state of residence** The transfer of customer records that pertain to a Child Support employee, either as a customer or authorised customer representative, must be arranged through a RACS Coordinator. This is an initiative by the Privacy Commission and will make sure there can be no conflict of interest or privacy incident. A customer cannot elect for this not to apply.
4	**RACS customers are not to be afforded special treatment, other than in the restriction of access to their information** RACS customers are required to fulfil their child support obligations and are not to be excluded from compliance or other activities. Staff who are customers must not use their position to influence decisions on their case or to gain preferential service. Doing so may be considered to be internal fraud.
5	**Access to RACS information is to be limited to the absolute minimum number of staff required for operational purposes** Restricting the number of staff with access to the data preserves the security of information.
6	**Only authorised staff are to access RACS information** Authorised staff are those whose duties require access to RACS information for official purposes and who have been explicitly authorised through the RACS access approval process. Staff who are to be authorised must be familiar with the policies and procedures contained in this document. RACS officers must not pass the restricted information onto a non RACS officer. Only staff with RACS access and a need to know may access this information, regardless if it is electronic or in paper form.
7	**All RACS information must be managed in accordance with the Information Security Policy** RACS officers must be familiar with procedures of how to classify, manage, store, move and destroy security classified information. Printing and copying of RACS information is to be kept to an absolute minimum. Unless authorised by Services Australia Security Branch no RACS 2 or 3 information can be removed from a Services Australia site.
8	**Electronic RACS information can only be stored or processed on Services Australia networked computers** Computer systems used to store and process RACS information must remain under the control of the agency. RACS information must not be stored on a network drive that does not provide access audit. RACS information must not be downloaded via a transfer stations, USB device or by email to an address outside the Services Australia network

Communications Protocols for RACS customers

Table 3: Reasons for RACS restrictions vary based on individual circumstances. The reasons is often sensitive, and may relate to a risk of harm to individuals.

Role	**Communication**
Non RACs officer Primary RACS customer	Most primary RACS customers will know why access to their information is restricted. If they ask what RACS actually means, use the following script to explain to the customer s47E(d)
Non RACS officer RACS by association	Usually, these customers will not know they are RACS or what this means. **Do not** tell the customer their details are RACS. If the customer asks why the person who answered the phone cannot help with their questions, use the following script. s47E(d) If the customer insists their simple question is answered. Tell them: s47E(d)
RACS officer All RACS customers	RACS officers need to exercise judgement as to what details they tell customers. Exercise a high level of discretion when the customer is not the primary RACS customer. Avoid disclosing details which: • may compromise the safety of the other customer, or other individuals, and • reveals personal information about another individual
RACS officer Primary RACS	**Primary RACS customers who know the reason for their RACS status** Explain to the customer, measures are taken to protect their sensitive information. Tell the customer that they too can protect their own details and enhance their personal safety. Effective security measures may be obtained from their local police Crime Prevention and/or Neighbourhood Watch section.
All Staff	**Customer discloses they are in Witness protection** Do not document this in Cuba, refer to Witness Protection information.

s22

Australian Government

Services Australia

Administration of Restricted Access 104-06020000

Currently published version valid from 23/06/2025 3:01 PM

Background

s22

This document outlines the processes that the National Restricted Access Team (NRAT) and Restricted Access Manager undertake to manage a Restricted Access customer and their record.

Authorised officers for Restricted Access

Each Restricted Access customer will have one Restricted Access Manager and at least one and up to three Restricted Access Officers in the National Restricted Access Team (NRAT) or at their home service centre authorised to access their customer record.

The NRAT or Restricted Access Manager may approve temporary access for a period of up to 7 days to specialist staff who need access for specific purposes, for example, Authorised Review Officers (ARO), Compensation, Debt Recovery, Business Integrity Service Officers and Claims staff. Each Restricted Access customer can have a maximum of one Temporary Officer at any time. A Temporary Officer is located within the agency.

Restricted Access customer changes address

Where a Restricted Access customer is managed by their local service centre and moves to another address that is not within the current service centre boundary, a change of contacts is required. The Process page outlines how to process the move.

If the customer is temporarily moving interstate, a change of contacts is not required. The customer can continue with their existing Restricted Access arrangements. If required, the Restricted Access Manager can add a Temporary Officer to the record to assist the customer at their nearest service centre if required. **Note:** this Temporary Officer assistance can only be for a maximum of 7 days.

The Resources page contains a link to the National Restricted Access page, which has relevant information for Restricted Access.

Related links

Restricted Access and eligibility

Support, maintenance and FAQs for Restricted Access

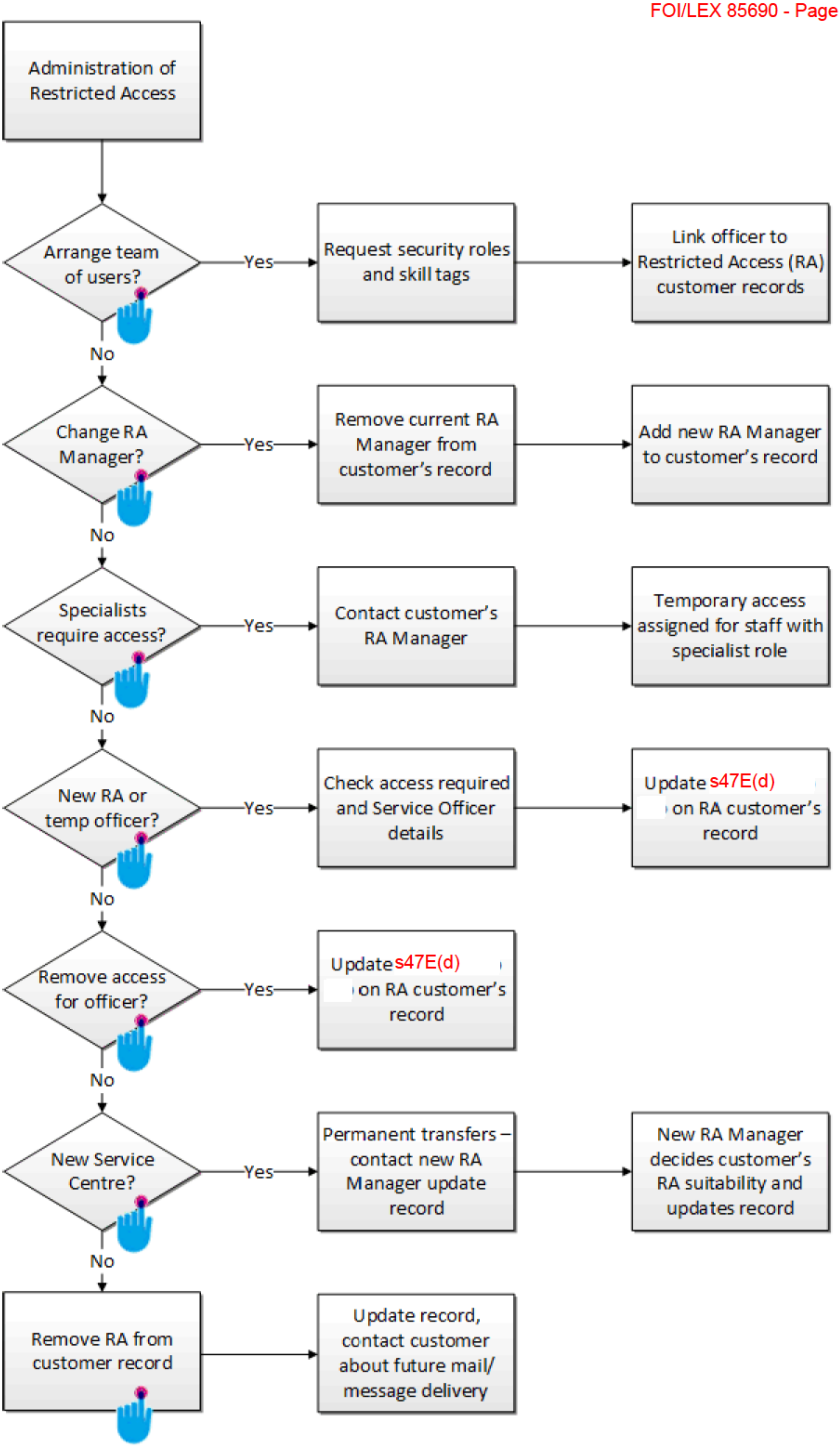
Process Summary

Flowchart

Administration of Restricted Access

This image provides a summary of the processes for the National Restricted Access Team (NRAT) and Restricted Access Manager role in administering Restricted Access.

Note: a text based version of the following process summary image is available.


Administration of Restricted Access
Arrange team of users?
Yes
Request security roles and skill tags
Link officer to Restricted Access (RA) customer records
No
Change RA Manager?
Yes
Remove current RA Manager from customer's record
Add new RA Manager to customer's record
No
Specialists require access?
Yes
Contact customer's RA Manager
Temporary access assigned for staff with specialist role
No
New RA or temp officer?
Yes
Check access required and Service Officer details
Update s47E(d) on RA customer's record
No
Remove access for officer?
Yes
Update s47E(d) on RA customer's record
No
New Service Centre?
Yes
Permanent transfers – contact new RA Manager update record
New RA Manager decides customer's RA suitability and updates record
No
Remove RA from customer record
Update record, contact customer about future mail/ message delivery

Process

This document outlines the processes that the National Restricted Access Team (NRAT) and Restricted Access Manager undertake to manage a Restricted Access customer and their record.

On this page:

Access for authorised users

Changing the RA Manager within the same service centre

Temporary access to a Restricted Access customer's record

Transfer of a Restricted Access customer from one service centre to another

Removal of Restricted Access from a customer's record

Restricted Access (RA) work items

Recording a Restricted Access application

Assessment of application by Restricted Access manager/APS6 Business administrator

Access for authorised users

Table 1: this table describes the process for the National Restricted Access Team (NRAT) and Restricted Access Managers to set up a team of authorised users of Restricted Access.

Item	Description
1	**Request the required security roles** + Read more ... **New Restricted Access Managers** Submit a request for s47E(d) within s47E(d) . This request must be approved by their line manager and the role owner. See Accessing and personalising Customer First for more information. **Access and Temporary Officers** At least one and up to 3 Access Officers are required to be assigned to a Restricted Access customer. All users must have s47E(d) or s47E(d) business role beforehand. Submit a request for s47E(d) within s47E(d) for staff who will be authorised to access any restricted customer records under their control. This request must be approved by their line manager and the role owner. s47E(d) These officers will be known as Temporary Officers and must be APS3 or above, in line with current business practice. See Accessing and personalising Customer First for more information.
2	**Request the required Skill Tags** + Read more ... **Restricted Access Managers** Restricted Access Managers who do not have a s47E(d) Skill Tag approved must submit a request in s47E(d) for the s47E(d) Skill Tag for approval by their line manager. This allows search results of restricted records assigned to the Restricted Access Manager to be viewed while the search results will be hidden for other users. **Note:** the user must not have both s47E(d) and s47E(d) assigned at the same time. **Temporary Officers**

	Temporary Officers who did not have a s47E(d) Skill Tag approved before 4 September 2015 require the s47E(d) Skill Tag assigned to them in s47E(d) Specify the required start and end dates, remembering that Temporary Officers should not be given access for more than 7 days. The approving officer for s47E(d) Skill Tag is their line manager. This will allow search results of restricted records to be displayed to authorised officers while the results will be hidden for other users. **Note:** other Restricted Access Skill Tags are not to be assigned to staff, as they are to be used for Child Support implementation of Restricted Access. The 'Create Skill tag' task card in s47E(d) is available for guidance on requesting Skill Tags for staff. The Resources page contains a link to the task card. From the task card: s47E(d) Once the s47E(d) Skill Tag has been approved, the NRAT or Restricted Access Manager must link the Temporary Officer to all relevant Restricted Access customer records. **Note:** once approved, provisioning of these resources happens overnight. When the request is approved in s47E(d) send an email to NRAT for temporary access to be coded on the customer record.

Changing the RA Manager within the same service centre

Table 2: This table outlines how to replace an existing Restricted Access (RA) Manager with another RA. Only staff with RA Business Administrator access can do the update

Step	Action
1	**Access the customer's record** + Read more ... If the customer's moves to another site or the RA manager role is going to another staff member a change of contacts is required. If using: • Process Direct, go to Step 2 • Customer First, go to Step 3
2	**Process Direct – update RA Manager** + Read more ... s47E(d) Go to Step 6.

3	**Customer First - Locate the current Restricted Access Manager in the record** + Read more ... s47E(d)
4	**Customer First - Remove the current Restricted Access Manager from the customer's record** + Read more ... s47E(d)
5	**Customer First -Add the new Restricted Access Manager to the customer's record** + Read more ... s47E(d)
6	**Finalise record** + Read more ... s47E(d)

Temporary access to a Restricted Access customer's record

Table 3

Step	Action
1	**Staff requirements for temporary access to a Restricted Access customer's record** + Read more ... Temporary access is not granted to Irregular and Intermittent (IIE) and Contractor staff. To be granted temporary access to a Restricted Access customer record staff must: • be a specialist. Specialist staff include: ∘ Authorised Review Officers (ARO) ∘ Compensation Service Officers ∘ Debt Recovery Service Officers ∘ Business Integrity Service Officers ∘ Claims staff • be at the APS3 level or above and • have the required Security Roles and Skill Tags, see Table 1. **Note:** if they do not have the Security roles and skill tags they can apply for them - it can take up to 24 hours for them to be applied Does the staff member have a specialist role, is APS3 or higher and have the required Security Roles and Skill Tags?

	- **Yes**, go to Step 3 - **No**, contact the National Restricted Access Team (NRAT) or Restricted Access Officers listed on the customer's record. These officers will need to process the particular enquiry. Procedure ends here
2	**Access the Restricted Access customer's record** + Read more ... Select the system being used: **Process Direct** + Read more ... s47E(d) Go to Step 3 **Customer First** + Read more ... s47E(d) Go to Step 3
3	**Update the Relationship details** + Read more ... Select the system being used: **Process Direct** + Read more ... s47E(d) Procedure ends here **Customer First** + Read more ... s47E(d)

	- **Note:** the default (and maximum) duration for a Temporary Officer is 7 days, but a fewer number of days can be chosen if required by adjusting the Skill Tag end date. They will automatically lose access to the Restricted Access customer's record - s47E(d) - Tell the newly appointed Temporary Officer that their access to the Restricted Access customer's record has been arranged Procedure ends here

Transfer of a Restricted Access customer from one service centre to another

Table 4

Step	Action
1	**Restricted Access customer changes address** + Read more ... The **losing** Restricted Access Manager must firstly action the record when a Restricted Access customer: - moves to another address that is not within the current service centre boundary and - is managed by their local service centre Is the customer moving temporarily? - **Yes**, advise the customer that their current Restricted Access arrangements will remain in place. Update the customer's address details. Procedure ends here - **No**, go to Step 2
2	**Customer moving permanently** + Read more ... Is the customer moving interstate? - **Yes**, an interstate environment transfer is required first. See Inter-environment change of address (ICoA) transfer of a customer record. Once the transfer has been actioned, return to this procedure. Go to Step 3 - **No**, go to Step 3
3	**Contact the new Service Centre Manager and update the customer's record** + Read more ... Check the customer's new address and contact the relevant Service Centre Manager for the service centre responsible for the customer's new location by phone. Send an email to National Restricted Access Team with the relevant details. Complete the steps below while on the phone with the gaining Service Centre Manager. Select the system being used: **Process Direct** + Read more ... s47E(d) **Customer First** + Read more ... s47E(d)

	s47E(d)
4	**Gaining Service Centre Manager action** + Read more ... Remain on the phone with the losing Restricted Access Manager until completion of the following steps. If using: • Process Direct, go to Step 5 • Customer First, locate the customer's Restricted Access Application: s47E(d)
5	**Determine if Restricted Access is suitable at new address** + Read more ... Assess if Restricted Access is suitable for the customer as a change of location may remove the requirement. Check Notes and the s47E(d) screen on the customer's record for any Notes/**DOC**s related to the change of address and view the customer's previous Restricted Access Application for the reason Restricted Access was approved. Is Restricted Access appropriate for the customer at the new address? • **Yes**, go to Step 7 • **No**, go to Step 6
6	**Restricted Access is rejected** + Read more ... Select the system being used: **Process Direct** + Read more ... s47E(d) Go to Step 9 **Customer First** + Read more ... s47E(d)

	Go to Step 9.
7	**Restricted Access is to continue accepted** + Read more ... The customer's record will remain restricted and can only be access by the National Restricted Access team and the nominated Temporary Officers s47E(d) • A review will be set for 12 months in advance by default • Clear out of the customer's record and wait a couple of minutes before accessing the customer’s record again **Note:** if the customer has a partner or other customers live with the protected customer, Restricted Access is to be applied to their records to protect the customer's whereabouts. Advise losing Restricted Access Manager that Restricted Access is accepted. Losing Restricted Access Manager, go to Step 8 Gaining Restricted Access Manager, go to Step 9.
8	**Losing Restricted Access Manager** + Read more ... Transfer of customer's paper file If the customer's Restricted Access application is: • **not accepted**, return the customer's paper file to the Records Management Unit (RMU) • **accepted**, the customer's paper file must be sent to the gaining Restricted Access Manager clearly marked s47E(d) The s47E(d) form must be completed and attached to the top of the file. Notify the Records Management Unit (RMU) via the Records Management service request web form that the paper file is being transferred. The Resources page contains a link to the web form Contact the customer to confirm their record has been transferred to the service centre for their new location, their Restricted Access status is being/has been assessed by the gaining Restricted Access Manager and that the gaining Restricted Access Manager will provide their new contact details. Procedure ends here.
9	**Gaining Restricted Access Manager** + Read more ... Contact the customer to confirm their record has been transferred to their service centre. If the customer's Restricted Access application is: • **not accepted**, advise the customer ◦ that their application for Restricted Access has been rejected and that they may discuss the decision with the Restricted Access Manager or pursue other avenues such as the Commonwealth Ombudsman ◦ of the security measures in place, including 100% logging of staff access to records. Refer them to the Services Australia website for privacy information. The Resources page contains a link to the Services Australia website ◦ about future delivery of online letters and messages. See Step 3 in Table 7 • **accepted**, see Restricted Access and eligibility for advice to the customer about the new arrangements Once the customer's paper file is received, securely store the file in a lockable cabinet, safe or other suitable location.

Removal of Restricted Access from a customer's record

Table 5: this table describes the process for the National Restricted Access Team (NRAT) or a Restricted Access Manager to remove Restricted Access from a Restricted Access customer record.

Step	Action
1	**Access the customer's record** + Read more ... A Restricted Access customer's circumstances have changed and they no longer require Restricted Access to their record. Select the system being used **Process Direct:** + Read more ... s47E(d) Go to Step 3 **Customer First**: + Read more ... s47E(d)
2	**Update the Restricted Access Application** + Read more ... s47E(d) s47E(d)
3	**Check delivery of mail and messages for the customer** + Read more ... Check if the customer receives their letters online. s47E(d) - If the customer does not have a myGov account, or their Centrelink account is locked or not linked, see How users create a myGov account and link services or Using the myGov Linking Application to help customers access services via myGov Ask the customer if they would like to subscribe to Centrelink Electronic Messaging. See Centrelink letters online and Electronic Messaging. Ensure that the customer’s contact details are current, including: - home and postal addresses - mobile phone number and - email address s47E(d)

Restricted Access (RA) work items

Table 6

Item	Description

1	**Process Direct - access and action RA work items** + Read more ... Only staff with appropriate access will be able to search s47E(d)
2	**Customer First - access and action RA work items** + Read more ... This function is available to RA Managers and RA Administrators only. s47E(d)

Recording a Restricted Access application

Table 7

Step	Action
1	**Restricted Access applications** + Read more ... If the National Restricted Access Team determines that Restricted Access is appropriate for the customer, the Restricted Access officer submits a Restricted Access Application in either: • Process Direct, go to Step 2 • Customer First, go to Step 3
2	**Creating a Restricted Access application - Process Direct** + Read more ... In the customer's record: s47E(d)

	s47E(d) Go to Step 4.
3	**Creating a Restricted Access application - Customer First** + Read more ... In the customer's record: s47E(d) The Restricted Access Application will workflow to the National Restricted Access Team as recorded on the s47E(d) screen. The National Restricted Access Team or the Restricted Access Business Administrator security role can select the application and finalise the application.
4	**Tell the customer their application will be considered and to expect phone contact** + Read more ... Where an assessment cannot be made immediately, the National Restricted Access Team will contact the customer by phone (from a private number) to advise of the decision. Tell the customer if the Restricted Access is granted: • If the customer has a partner, Restricted Access will also be applied to the partner’s record. This is because the customer's information is accessible via the partner’s record • Other customers who reside with the protected customer may also need to have Restricted Access applied to protect the customer's whereabouts If the **application is granted**, the customer will be asked to provide a verbal declaration of their acceptance of Restricted Access Acknowledgement obligations. Remind the customer:

	• Restricted Access will not preclude them from the normal requirements for the payment type, including reviews. s47E(d) • access for self service, online letters and Electronic Messaging need to be considered and locked or unsubscribed as required. To lock self service, see Centrelink self service access status, locking and unlocking If the **application is not successful**, tell the customer they may discuss the decision with the National Restricted Access Team Manager or pursue other avenues such as the Commonwealth Ombudsman. To assess and finalise an application, go to Table 8.

Assessment of application by Restricted Access manager/APS6 Business administrator

Table 8

Step	Action
1	**Access Restricted Access Application** + Read more ... **Process Direct** s47E(d) **Customer First** s47E(d) Check that a postal address is recorded for the customer. Determine if Restricted Access is suitable for the customer. Is Restricted Access suitable for the customer? • **Yes**, go to Step 2 • **No**, go to Step 4
2	**Read Restricted Access obligations and get verbal declaration from customer** + Read more ... Phone the customer and read them the verbal declaration - Customer Restricted Access acknowledgement script: s47E(d)

	s47E(d) Does the customer accept their Restricted Access obligations? - **Yes**, go to Step 3 - **No**, go to Step 4
3	**Restricted Access is granted** + Read more ... **Process Direct** s47E(d) **Customer First** s47E(d) s47E(d) For help to add a Restricted Access officer, see Administration of Restricted Access. Go to Step 5.
4	**Restricted Access is rejected** + Read more ... Advise the customer their application for Restricted Access has been rejected and that they may discuss the decision with the Restricted Access manager or pursue other avenues such as the Commonwealth Ombudsman. **Process Direct**

	s47E(d) **Customer First** s47E(d) Procedure ends here.
5	**Create Note/DOC and tell customer their record is restricted** + Read more ... Create a closed **Note/DOC**. s47E(d) **Confirm** Tell the customer their record is now restricted and can only be accessed by authorised officers and other authorised temporary officers. Does the customer have a partner? - **Yes**, go to Step 6 - **No**, procedure ends here
6	**Check partner's postal address** + Read more ... In the partner's record, check if the partner has a current postal address (POS). If not recorded, add a postal address. **Note:** Restricted Access will not apply correctly to the partner's customer record if a postal address is not recorded. Create and grant Restricted Access in either: - Process Direct, go to Step 7 - Customer First, go to Step 8
7	**Create and grant Restricted Access on partner's record - Process Direct** + Read more ... s47E(d)

	s47E(d) Procedure ends here.
8	**Create and grant Restricted Access on partner's record - Customer First** + Read more ... s47E(d)

Resources

Services Australia website

Your right to privacy

Online security

Forms (Staff)

SS354   Customer Deny Access acknowledgement

SS355   File Movement for Deny Access Customer

Intranet links

Records Management service request mySupport form (mySupport form title: CREATE, TRANSFER OR RETRIEVE A CORPORATE FILE).

National Restricted Access

Skill Tag and Access Request

Contact details

Restricted Access

s22

Australian Government

Services Australia

Support, maintenance and FAQs for Restricted Access 104-06030000

Currently published version valid from 27/11/2024 9:46 PM

Background

s47E(d)

This document outlines monitoring and reviewing Restricted Access customers, Quality On Line (QOL) for Restricted Access customer activities, Frequently Asked Questions (FAQs), and hints and tips in monitoring Restricted Access cases to ensure they are current and correct.

The Resources page contains FAQs, links to the Services Australia website and the National Restricted Access page, which has relevant information for Restricted Access.

Related links

Restricted Access and eligibility

Administration of Restricted Access

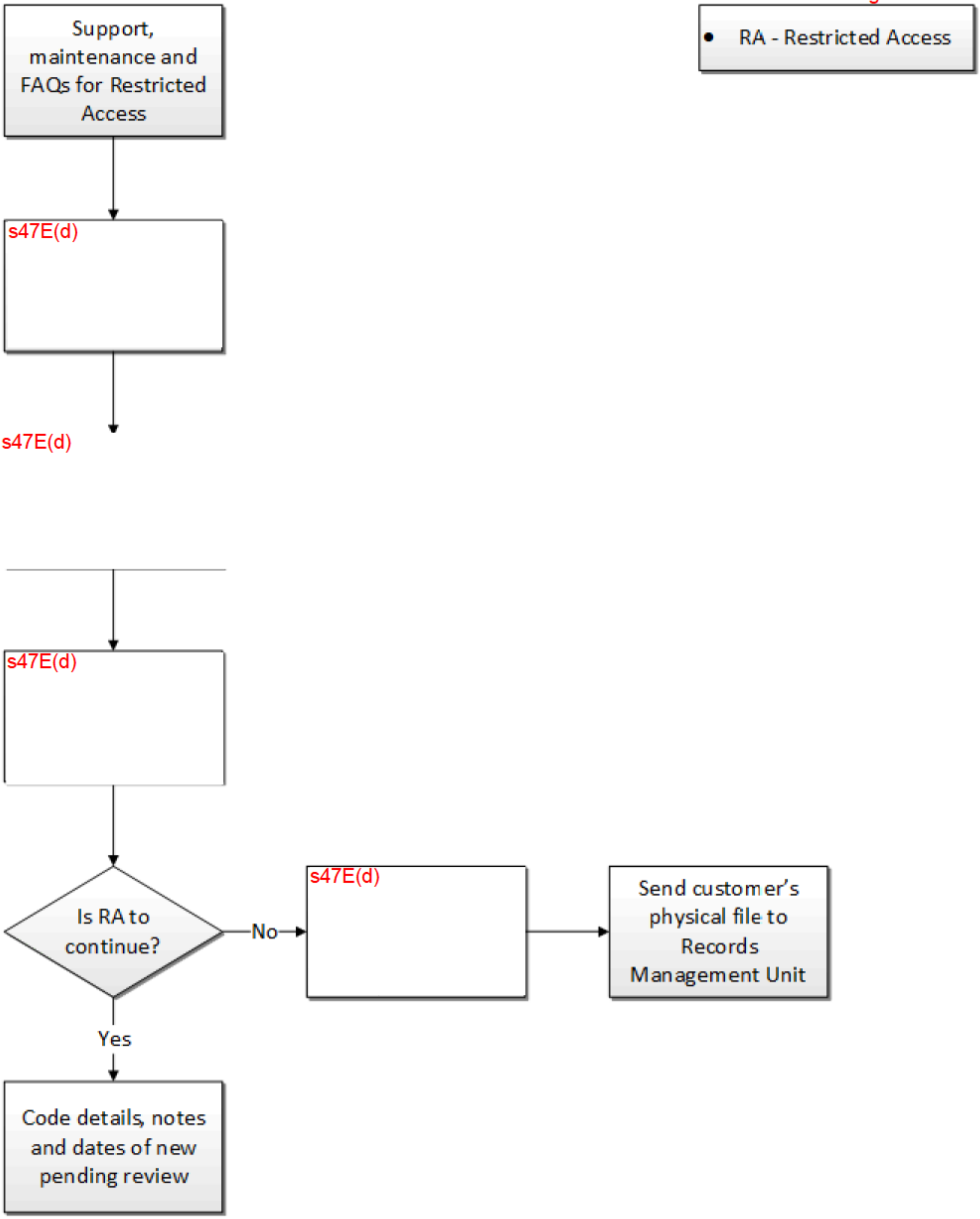
Process Summary

Flowchart

Coding Restricted Access reviews

This image provides a summary of the process to update and complete a Restricted Access review.

Note: a text based version of the following process summary image is available.


● RA - Restricted Access
Support, maintenance and FAQs for Restricted Access
s47E(d)
s47E(d)
s47E(d)
Is RA to continue?
No
s47E(d)
Send customer's physical file to Records Management Unit
Yes
Code details, notes and dates of new pending review

□

Process

This document outlines monitoring and reviewing Restricted Access customers, Quality On Line (QOL) for Restricted Access customer activities, Frequently Asked Questions (FAQs), and hints and tips in monitoring Restricted Access cases to ensure they are current and correct.

On this page:

Searching for Restricted Access customers within an Org Unit

Conducting reviews for Restricted Access customers

Coding Restricted Access reviews in Process Direct

Coding Restricted Access reviews in Customer First

Quality On Line (QOL) for Restricted Access customers   submitted activity approval process

Information about technical and system support for Restricted Access customers

Searching for Restricted Access customers within an Org Unit

Table 1: this table describes how to search for Restricted Access customers within an Org Unit to ensure Restricted Access arrangements are reviewed and maintained correctly.

Step	Action
1	**Monitoring and searching for Restricted Access customers** + Read more ... Part of the National Restricted Access Team and Restricted Access Manager's role is to ensure the Restricted Access customers are being maintained and reviewed appropriately. This involves regularly reviewing the current Restricted Access customer's circumstances, and that the authorised officers for each record are current and appropriate. The ongoing need for each record to be restricted should be reviewed based on the customer's individual circumstances. See Table 2 Conducting reviews for Restricted Access customers. Search for Restricted Access customers within an Org Unit in Customer First, go to Step 2. Available Restricted Access searches in Customer First and Process Direct, go to Step 5.
2	**Obtaining a list of current Restricted Access customers for Org Unit in Customer First** + Read more ... Staff must ensure they are not in any customer records in Customer First. s47E(d) The list of Restricted Access customers for the site will be displayed. s47E(d) **Note:** this search is performed by the Restricted Access Manager for the particular Org Unit, as they should have access to all the records associated with the Org Unit. If they are not the Restricted Access Manager for Restricted Access customers held at their Org Unit, the customer record will display as s47E(d) and the Manager will not have access. The Restricted Access Manager for the record should be contacted and the record transferred out to the appropriate service centre or the Restricted Access Manager corrected. The same principle applies if a Restricted Access Officer conducts the above search for a particular Org Unit. **Note:** only customer records the searcher is authorised to access will display, the others will be replaced with s47E(d)
3	**Obtaining a list of outstanding Restricted Access Applications** + Read more ... **Note:** status is **RA assessed** or **pending** security for an Org Unit. s47E(d)

	s47E(d) **Note:** only customer records the user is authorised to access will display. Other records will display as s47E(d) The list of outstanding Restricted Access or pending security applications for the site will be displayed. **Note:** customer applications for Restricted Access are required to be approved within 3 days.
4	**Obtaining a list of outstanding Restricted Access reviews for Org Unit** + Read more ... s47E(d) s47E(d) **Note:** only customer records the user is authorised to access will display. Other records will display as s47E(d) The list of Restricted Access reviews for the site will be displayed. **Note:** Restricted Access customers should be reviewed based on the customer's individual circumstances. See Table 2 Conducting reviews for Restricted Access customers for more information. Procedure ends here.
5	**Available Restricted Access searches in Process Direct and Customer First** + Read more ... A number of Restricted Access searches are available by updating the s47E(d) field on the s47E(d) s47E(d) screen. These include: s47E(d) s47E(d)

Conducting reviews for Restricted Access customers

Table 2: For National Restricted Access Team (NRAT) or the Restricted Access Managers only

Item	Description
1	**Role of the National Restricted Access Team (NRAT) and the Restricted Access Manager** + Read more ... The role of the National Restricted Access Team (NRAT) or the Restricted Access Manager includes conducting reviews of Restricted Access customers to assess if there is a continuing need for Restricted Access. See Administration of Restricted Access for more information about the role of the NRAT or a Restricted Access Manager.
2	**Reasons to conduct a review of Restricted Access** + Read more ... Review Restricted Access customers based on their individual circumstances to ensure the additional level of protection is still required. If the customer is managed by their local service centre and the customer relocates to a different service centre: • the Restricted Access should be removed • review the customers continued need for Restricted Access, given the change of circumstances, before Restricted Access is reapplied

	• reapply/reject Restricted Access at the gaining service centre See Administration of Restricted Access for actioning a change of Restricted Access Manager
3	**Preparing for a Restricted Access review** + Read more ... The NRAT or Restricted Access Manager should: • review any notes on the customer's record. **Note:** physical files are only held at service centres if the customer is managed by them • invite the customer, either by phone or mail, to discuss their situation. If using mail create a Q888 letter inviting the customer to initiate contact via phone If the customer has not contacted within a reasonable timeframe, either: • send a Request for Information (RFI) letter or • review the customer's Restricted Access based on information held on their record. **Note:** extreme caution should be exercised before removing the customer's Restricted Access. In no circumstance will Restricted Access be permanently removed without notifying the customer (verbally or in writing).
4	**Conducting a Restricted Access review** + Read more ... The NRAT and Restricted Access Managers should assess each customer's eligibility for Restricted Access on an individual basis. See Restricted Access and eligibility. s47E(d) The NRAT and Restricted Access Managers, during the review should: • remind customers of the limitations that Restricted Access will have on their dealings with the agency • discuss alternative security arrangements available • check and discuss self-service option • ensure the customer still wishes to retain Restricted Access on their record. For more information on explaining Restricted Access to customers, customer obligations, and alternative options, see Restricted Access and eligibility. Once the customer's eligibility for Restricted Access has been determined, a note documenting the outcomes and discussion should be placed on file and documented on the customer's record. If Restricted Access has been removed at the customer's request, a signed statement from the customer advising this should be obtained. In all cases, the customer must be notified in writing of the removal of Restricted Access.

Coding Restricted Access reviews in Process Direct

Table 3

Step	Action
1	**Access the Restricted Access customer's record** + Read more ... s47E(d)

2	**Locate the Restricted Access review** + Read more ... s47E(d)
3	**Updating the Restricted Access Review Details screen** + Read more ... s47E(d) Is Restricted Access going to be ceased? • **Yes**, see the Removing Restricted Access from a customer's record table in Administration of Restricted Access • **No**, procedure ends here

Coding Restricted Access reviews in Customer First

Table 4:

Step	Action
1	**Access the Restricted Access customer's record** + Read more ... s47E(d)
2	**Locate the Restricted Access review** + Read more ... s47E(d)
3	**Updating the Restricted Access Details screen** + Read more ... s47E(d) Is Restricted Access to continue? • **Yes**, go to Step 4

	• **No**, go to Step 5
4	**If Restricted Access is to continue** + Read more ... s47E(d)
5	**If Restricted Access is to cease** + Read more ... s47E(d) **Note:** a letter should be provided to the customer confirming they requested Restricted Access to be removed or confirming this has occurred. • If the customer's physical file is held at a service centre, it should be sent to the Records Management Unit (RMU)
6	**Final Restricted Access review checks** + Read more ... Check on the s47E(d) tab that the Restricted Access Manager, Officers and service centre are correct if the Restricted Access is to continue. The staff listed on this screen should match those listed on the s47E(d) screen. If they do not, this should be investigated. s47E(d) Staff listed as Restricted Access Officers should also be reminded of their responsibilities as part of this role. For more information on the role of Restricted Access Officers, see Restricted Access and eligibility. Other checks include: • The s47E(d) field on the Restricted Access Application should always be filled with the name of the Restricted Access Manager for the listed service centre or National Restricted Access Team (NRAT). This field should be edited to insert or update the relevant staff member if it is blank or incorrect • When the flags for Restricted Access reviews are working correctly, they will flow to the inbox of the responsible officer. Therefore, it is essential for this field to be present and correct • Service centres should check all physical Restricted Access customer files held in the Manager's office at the site. These physical files should match the Restricted Access records in Customer First. Where the customer record is not restricted and the result of the Restricted Access Application has not been documented clearly, contact should be made with the customer to ensure this is a correct reflection of their current circumstances and needs • Files where the customer is not on Restricted Access or the Restricted Access customer is managed by the National Restricted Access Team (NRAT) should be sent to the Records Management Unit (RMU). Where the customer is on Restricted Access at another service centre, the file should be forwarded there

Quality On Line (QOL) for Restricted Access customers - submitted activity approval process

Table 5

Step	Action
1	**Access a customer's record** + Read more ... • A staff member with access to the customer's record will need to check the activity under the s47E(d) process in Customer Record. **Note:** this must be a different staff member to the person who submitted the activity • The staff member does not require QOL access to approve the activity, although they should have the necessary competence to be able to assess that the coding is accurate and correct • If no staff members with the necessary skills have access to the customer record, a second party (with the required skills) should be used and permitted to supervise and observe the approval process for this short duration. This should be annotated in the Notes section Go to Step 2 for more details on how to code.
2	**Checking work in** s47E(d) + Read more ... s47E(d) • Fully check the source documentation of **DOC** against each screen in the screen flow and determine if the work is correct against the Four Pillars of Payment Correctness and the Minimum Standards, before finalising the check at the end of the screen flow

Information about technical and system support for Restricted Access customers

Table 6: this table describes additional technical/system support to access a Restricted Access customer's record.

Item	Description
1	**Technical/system support staff** + Read more ... Occasionally staff need to access the expertise of technical/system support staff in order to provide accurate information or code required updates on a customer's record. All staff in Services Australia are bound by privacy and secrecy laws that control how the information the agency administers can be collected, used and/or disclosed. The Restricted Access service is not required by legislation but is a service the agency offers as an additional layer of security to customers who feel their records need additional protection for a variety of reasons.
2	**Screen sharing** + Read more ... Screen sharing customer records is allowed where there is a legitimate business requirement. Should additional technical/system support be required on a customer with a Restricted Access record, screen sharing is allowed in the following circumstances: • The customer is present and gives permission. The screen sharing is to be documented to provide a trail detailing the logon of staff members being shared with and the reasons for screen sharing

	- The customer is unavailable and the Restricted Access Manager's permission has been obtained. The screen sharing is also to be documented to provide a trail detailing the staff member/s logon and the reasons for screen sharing
3	**Access required for a longer period of time** + Read more ... If a third party staff member needs access to the record for longer than guidance or verbal support, e.g. coding to fix the record, then temporary access should be requested as per normal Restricted Access procedures. Restricted Access may be granted at the National Restricted Access Team's or Restricted Access Manager's discretion. This access is then logged as per normal. **Example:** a Restricted Access customer attends their local service centre to ask about an advance. The customer has an outstanding debt preventing access to the advance. To provide correct information, the authorised Restricted Access Officer needs the technical expertise of a member of the Debt Team. Having obtained the customer's permission, screen sharing is done to allow accurate information to be given to the customer. The record is documented to reflect the customer contact, information provided and screen share access of the Debt Team staff member via their logon ID. Following this information, the customer then requests a review of the debt. This request is sent to the Debt Team. A member of the Debt Team now requests temporary access to the customer record to respond to the review request and provide any necessary coding or updates to the record.

Resources

For FAQs and answers, see the National Restricted Access page.

Services Australia website

Your right to privacy

Scams and identity theft

Contact details

See contact details for Restricted Access Business Administrators in Restricted Access.

Intranet links

Records Management service request mySupport form (mySupport form title: CREATE, TRANSFER OR RETRIEVE A CORPORATE FILE).

National Restricted Access

Skill Tag and Access Request