s 22

Australian Government

Services Australia

Managed Service Plan (MSP) - Reviewing 104-07050050

Currently published version valid from 18/11/2025 8:19 PM

Background

s 22

This document outlines the process staff use to review an MSP and record the outcome.

MSP reviews

An MSP is reviewed to assess any ongoing risk posed by the customer and the suitability of transitioning a customer back to standard service channels.

The outcomes of a review may be to:

- implement a longer term MSP following a provisional MSP
- end an MSP and return the customer to standard service channels
- extend an MSP unchanged
- vary the arrangements in place and set a new review date

MSPs are managed through the Customer Incident Management System (CIMS) for:

- all Centrelink customers
- Medicare Public customers (proactive MSP with restrictions)
- Some Child Support customers, if there is an identified risk to other service brands

All MSPs for Health Service Delivery professionals are recorded in the Customer Incident Recording Tool (CIRT).

For information about MSP timeframes, see Customer aggression - MSP.

Triggers for MSP reviews

An MSP is reviewed when:

- the MSP is due to end
- the customer requests a review
- there is a significant change in a customer's circumstances
- when there is an escalation in aggressive behaviour or the customer is non-compliant with their restrictions
- when a decision is made to change the servicing arrangement
- Personalised Services (PS) manage the MSP as a proactive direct referral, and PS has addressed the MSP servicing strategies and reason for the referral

For **Centrelink** customers, the review process will be automatically initiated. There is no automatic extension of an MSP.

If a review is not undertaken, the MSP will automatically cease on the End Date without a documented assessment of any ongoing risk. The customer will return to standard/ mainstream servicing arrangements unless a decision is made to extend or vary the MSP.

The Employee Responsible and One Main Contact (OMC) get a system-generated email:

- 28 days before the MSP is due to end
- when an MSP has reached the end date without the review being done.

For **Child Support** customers, if an MSP is in place, Personalised Services Service Officers (PSSO) must set a reminder for 28 days before the end of the MSP.

Coordination of MSP reviews

The review of an MSP is coordinated by the Employee Responsible as part of the monthly Local Assessment Panel (LAP), Zone Assessment Panel (ZAP) or Health Service Delivery Division (HSDD) Assessment Panel meeting in discussion with all relevant parties including the One Main Contact (OMC) or PSSO and other specialist officers. Customer Aggression Operational Contact (CANOC) coordinates and performs the secretariat functions for the Zone Assessment Panel. For more information on LAPs and ZAPs, see Customer aggression Managed Service Plan.

The Employee Responsible records a recommendation for the Approver.

See Resources for a link to Customer aggression prevention networks and stakeholders.

Customer input into MSP reviews

Customers must be given the opportunity to have input into the review. There are limited instances where a customer may not be invited to participate. Alternative methods of review may be considered for these cases.

Resources has letter templates.

Requesting support

Staff can ask for support from CANOC or Customer Aggression Prevention Team (CAPT) when reviewing an MSP. Resources has a link to their contact details.

Warning message alerts staff

Staff are alerted to a customer's MSP when accessing the customer record.

For **Centrelink** customers, the Customer Incident Management System (CIMS) warning message pops up displaying information when an active Services Australia MSP is in place for:

- Services Australia
- Employment Services Provider MSPs

Note: where Services Australia does not have an active MSP in place, the Provider MSP will not result in the display of the warning message in Customer First, Process Direct or the FoH Application.

Provider MSPs do not impact the way a customer can deal with Services Australia, and are for information only. This information is of value when giving advice to customers on dealing with their provider and identifying potential risk to the safety of Services Australia staff.

For **Medicare** customers, a Sensitive Information alert pops up in the Consumer Directory Maintenance System (CDMS) when a customer has an active **Sensitive Information alert** for **Full or partial service restrictions**.

Staff can view the MSP details in the indicator in the Sensitive Information pop up table or tab.

See Sensitive Information Indicators in the CDMS for more details.

For **Child Support** customers, a warning message appears in Cuba identifying that Personalised Services manage the customer and a service restriction is in place. See Personalised Services.

Notification Alert

A customer with an MSP may also have a Notification Alert.

A Notification Alert will not carry over to a new MSP if it is extended or replaced. A new Notification Alert will need to be triggered if required.

The Resources page contains:

- MSP letter templates
- MSP SMS guide

- Service channel restrictions
- Contact details
- Services Australia webpages
- Intranet sites

Related links

Customer aggression   Prevention and management

Customer aggression   Response

Customer aggression   Staff Support

Customer aggression   Managed Service Plan (MSP)

Managed Service Plan (MSP)   Proposing, recording and approving

Managed Service Plan (MSP)   Implementing

Managed Service Plan (MSP)   Customer not complying

Managed Service Plan (MSP)   Customer service delivered through a One Main Contact (OMC)

Managed Service Plan (MSP)   One   off variation

Accessing and using the Customer Incident Management System (CIMS)

Notification Alert

Family and domestic violence

Providing services to customers with disabilities

Referring customers to and handling customer enquiries and correspondence for Personalised Services

National Redress Scheme overview

Nominee arrangements under Income Management

Reviewing nominee arrangements

Person Permitted to Enquire (PPE) or Update (PPU) authority

Sensitive Information Indicators in the CDMS

Process

This document outlines the process staff use to review an MSP and record the outcome.

On this page:

Reviewing an MSP

Record the review outcome and notify the customer

Record and approve the safety alert review outcome

Reviewing an MSP

Table 1: triggers for review, factors to consider, who is involved in the review, and requirements for inviting customers to participate in a review.

Step	Action
1	**Principles of decision making when reviewing an MSP** + Read more ...

	Decisions about an MSP must be based on the customer’s individual circumstances and requirements. Consider each situation on its merits, taking into account all available information. Throughout the following steps, use these principles of decision making. - Apply procedural fairness. Give a reasonable timeframe for the customer to contribute to the review - Make sure the process is free of bias. It may not be appropriate for a person who was affected by an incident to be involved in the review - Gather evidence to support a decision without personal opinion or assumptions. Give sufficient weight to the relevant facts - Address matters in dispute the customer has a right to request a review with genuine consideration
2	**Who should be part of an MSP review** + Read more ... Appropriately skilled staff should be involved in the review. Include the One Main Contact (OMC) or Personalised Services Service Officer (PSSO) in the review. For more information about the role of the OMC/PSSO in the MSP review see the Background page. The review may occur at the Zone Assessment Panel (ZAP), HSDD Assessment Panel meeting, which is coordinated by the Customer Aggression Network Operational Contact (CANOC) or Local Assessment Panel (LAP) coordinated by local leadership. Contribution to the review can also be sought from: - specialist staff, such as a social worker or psychologist - representatives from other service delivery brands if the MSP relates to a mutual customer. This can include team leaders or managers - representatives from partner agencies, if the review relates to a joint MSP. This can include NDIA, ATO, DVA - a manager from the affected site (Service Centre or Smart Centre) - the relevant CANOC representative (Service Zone, Smart Centre, HSDD or other business areas) - a representative from the Customer Aggression Prevention Team (CAPT) If the review was triggered by a request from the customer, the review outcome should be approved by a staff member other than the original Approver of the MSP. The review Approver should be at the same level or a higher level than the original Approver. See Resources for links to: - CANOC and Customer Aggression Prevention contact details (Service Zone, HSDD and Smart Centre) - Local and Zone/HSDD Assessment Panel structures
3	**When a review of an MSP is initiated** + Read more ... Initiate a review when one of the following criteria is met. - The MSP is due to end. Go to Step 4 - The customer requests a review. Go to Step 5 - A significant change has occurred in a customer's circumstances or behaviour, such as: ◦ the customer is on a proactive MSP without restrictions and there is an indicator or incident of aggression that reflects the need to apply service restrictions because of an increased risk ◦ the conditions of the MSP have placed a customer in hardship. Go to Step 6 - Personalised Services has managed the customer and determined the risk has been addressed. The MSP no longer requires Personalised Services management. This decision will be based on an assessment of the future risk of aggression being mitigated - A current MSP customer is deceased. Add an end date to the MSP and a note with the reason for the review and end date. A notification letter is not required
4	**MSP is due to end** + Read more ... When the end date of an MSP is approaching, the agency will do a review. Allow enough time to make an informed decision to extend, vary or cease the MSP. **Automatic review is initiated by CIMS** 28 days before a long-term MSP ends, CIMS will send a reminder email to:

	• the OMC or PSSO • the Employee Responsible • Personalised Services The email will tell them that it's time to complete the review. **Note**: CIMS does not send a reminder about a provisional MSP. If no action is taken, CIMS sends a second reminder 2 days before the MSP is due to expire. Start the review on the same day the 'MSP expiring' email is received (28 days prior to the MSP expiry). This allows enough time to invite the customer to participate in the review. Go to Step 6.
5	**Customer asks for a review** + Read more ... A customer may ask for an MSP review at any time. Consider all requests on their merits. Some of the reasons for customer-initiated reviews include: • the customer experiences financial hardship as a result of the MSP • the MSP makes it difficult to meet obligations • an allegation of bias • the customer has experienced a significant change in circumstance • an allegation that the original decision was unreasonable • the customer was not provided with an opportunity to contribute to the review decision. The customer may be invited to provide further information about their circumstances so it can be considered during the review. **Repeated requests to review an MSP** If a customer makes frequent or persistent requests for review on the same grounds, and the agency has already made a determination, the agency can decide that the full review process will not be applied. This decision and the grounds for review must be documented in the MSP. Repeated requests may be considered counterproductive behaviour. If this happens, record an incident. See: • Reporting, recording and escalating incidents of customer aggression • Reporting, recording and escalating incidents of customer aggression - Medicare Go to Step 6.
6	**Invite the customer to participate in the review** + Read more ... The OMC/PSSO must attempt to contact the customer by phone to invite them to participate in the review. There are limited circumstances where it is not appropriate to phone a customer. Wherever possible contact the customer's Power of Attorney, nominee or person permitted to enquire (PPE) or update (PPU) where a decision is made not to contact the customer directly. In all instances where a decision is made not to contact a customer, the reasons must be documented in the MSP. **Centrelink - Nominees, PPE or PPU:** the MSP review process is also an opportunity to review existing voluntary nominee arrangements. An example is when family and domestic violence are a concern for the customer and the authorised person. For more information, see Reviewing nominee arrangements. If the phone contact is successful, the OMC/PSSO must tell the customer: • the agency is reviewing their MSP • the date and time of the review (re-negotiate this where required) • they must give supporting evidence or further information with adequate time to be included • how the review will be completed • when they can expect to hear about the outcome After the conversation with the customer: • the OMC/PSSO must record details of the discussion in the notes section of the MSP

	• if the customer verbally confirms their intention to participate in the review, a letter is not required. Document the conversation in the notes section of the MSP. Go to Step 7 If phone contact is not successful, notify the customer with a letter and SMS: • the OMC/PSSO must record any contact attempts in the notes section of the MSP • send the Invitation to participate in review letter to the customer. See Resources for the link • send an MSP review invitation SMS (approved decision makers only). See Resources for the text • give the customer enough time to respond to the letter (usually 14 days). This may vary depending on the customer's location Contact CAPT for support and advice where required. See Resources for contact details.
7	**Consider evidence** + Read more ... The OMC will provide the following input to inform the LAP/ZAP recommendation: • MSP review recommendation: extend/vary/cease • Rationale • Progress and/or outcome of each servicing strategy • Outstanding action items • Recommended service channel/s restrictions • Recommended servicing strategies • Proposed timeframe (if extending/varying) The LAP/ZAP conducts a comprehensive review of the current MSP, considering the following evidence: • the severity of the original incident • individual customer circumstances, such as their vulnerabilities, outstanding business • documents and notes on the MSP • the customer's willingness to engage with their OMC/PSSO • any triggers that may have contributed to the incident/s have been addressed • information provided by the customer • how the customer behaved during the review contact • the customer's behaviour since the MSP was implemented, for example, any new incidents of customer aggression or counterproductive behaviour, or improvements in behaviour • if the customer has adhered to any restrictions in the MSP • how the customer has responded to any servicing strategies and whether recorded timeframes, milestones or deadlines for servicing strategies have been met • any legal considerations that may impact on how the agency offers services to the customer. These could include: o incarceration (or other lawful custody) o psychiatric confinement o any pending charges o Intervention, Protection Orders and Apprehended Violence Orders. See Resources for more information about these kinds of orders • whether the customer has an ongoing need to contact the agency in a particular channel • if the customer's reason for contact that resulted in the MSP has changed • any other changes in customer circumstances • the OMC's input and recommendation **Note:** access call recordings if appropriate. See Call and screen recording - information and access. If the recommendation is to: • end the MSP, see Table 2 • extend or vary the MSP, go to Step 8
8	**Consider the timeframe for the new MSP** + Read more ... The timeframe for the MSP needs to be proportional to the customer's circumstances and the level of risk posed to Services Australia and others. If the customer has ongoing vulnerabilities and extra time is needed to complete servicing strategies, a longer term MSP is appropriate. The timeframe must allow for the servicing strategies to be addressed. Go to Step 9.

9 **Consider the end date of the proposed MSP when using CIMS** + Read more ...

The MSP ends automatically when the end date recorded in CIMS is reached. Carefully consider the end date to make sure the agency has enough time to make an informed decision from the initiation of the automatic review email in CIMS to the end date (28 days).

For example, consider any public holidays or other events that may impact the ability to appropriately review the MSP.

10 **Consider the type of MSP** + Read more ...

The type of MSP is either reactive or proactive.

A reactive MSP is one that follows an incident of customer aggression or counterproductive behaviour, including where the behaviour is directed at another customer.

A proactive MSP is one where a customer has:

- identified vulnerabilities or barriers
- displayed counterproductive behaviour that could pose a risk to staff safety
- been directly referred to Personalised Services after being identified as high risk after proactive data analysis,
- been directly referred from one of the following business areas:
    - Escalated or External Complaints
    - Media Branch
    - National Restricted Access Team (NRAT)
    - Senior Executives
    - Smart Centres
    - Social Work Services
    - Intelligence and Investigations

If the existing MSP is reactive and the risk to the agency has been mitigated, additional support may be required before the customer can return to mainstream services. In this case, consider implementing a proactive MSP.

Is the proposal for a reactive MSP?

- **Yes**, go to Step 11
- **No**, go to Step 12

11 **Consider service channel restrictions** + Read more ...

Full or partial service channel restrictions can be placed on each of the primary service channels for customer contact. If a channel is fully available, it means that the customer can access services normally through that channel.

Service channel restrictions apply consistently across all service brands - Centrelink, Medicare and Child Support.

Consider a partial service channel restriction if a full restriction of the service channel may:

- impact the customer's ability to meet their obligations to the agency
- negatively affect a customer experiencing vulnerability
- not support the customer in adhering to the MSP
- prevent the delivery of necessary services to the customer.

Resources page in Proposing and recording a MSP has tables showing the types and levels of service channel restriction.

12 **Consider servicing strategies and specialist consultations** + Read more ...

Review and update the progress/success of servicing strategies in the current MSP. Consider the need to continue or introduce new strategies for any future MSP.

Use indicators of potential vulnerability and risk issues to assess if it is appropriate to consult with or refer the customer to available resources, external service providers or agency specialist staff. Make a referral to the appropriate area if the customer needs specialised assistance.

The Family and Domestic Violence Support (FDVSM) Model supports staff to identify customers affected by family and domestic violence, see Family and domestic violence.

Servicing strategies

s 22 s 22

- Internal referrals, such as:
    - Appeals
    - Centrepay
    - Community Engagement Officers (CEO)
    - Change of Provider
    - Income Management
    - Indigenous Service Officer (ISO)
    - JCA or ESAt
    - JCA
    - Multicultural Service Officers (MSO)
    - Incarcerated Customer Services team
    - Social worker
    - Youth Specialist Agency
- External referrals, such as:
    - Anger management counselling
    - Drug and alcohol counselling
    - Financial counselling
    - Family Relationship Advice Line
    - Family Violence
    - Grief counselling
    - Housing/Accommodation
    - Legal Aid
    - Parent Support Service
    - Relationship service
    - Social or community program/course
    - Welfare agency
- Other strategies, such as:
    - Appointment of a nominee or person permitted to enquire (PPE)
    - Assess other payment types
    - Apology
    - Discuss behavioural expectations with customer
    - Email redirection
    - Telstra inbound call customisation
    - Proactive Contact
    - Consult with provider
    - Use of self service, apps or other
    - Weekly payments
    - Workplace Protection Order

See Managed Service Plan (MSP) - Proposing, recording and approving for details about the call customisation process

Use the Payment and Service Finder to locate the services most suitable to the customer and available in their local area. See Resources for a link to the Payment and Service Finder on the Services Australia website.

Note: an MSP does not require approval by the delegate if service strategies are being implemented and no service restrictions will be applied to the customer.

Specialist referrals

Specialist consultation may happen before or during the MSP.

The following specialist referrals are available in CIMS:

- Social Worker consulted
- Forensic Psychologist consulted
- Assessment Services consulted
- Multicultural Services consulted
- Legal Services consulted
- Customer Aggression Prevention Team consulted
- Indigenous Services consulted
- Incarcerated Customer Services team consulted
- Community Engagement Officer Network consulted
- Protective Services consulted
- Smart Centre Critical Response Team consulted
- Complaints

	- Referral to ACER team See Resources for links to each of these teams and services.
13	**Consider safety alert** + Read more ... When an MSP is being reviewed, a safety alert should be considered where an incident meeting the safety alert criteria has been recorded at any time. The decision to implement a safety alert is separate to the decision to implement an MSP. The customer **must** have an active MSP for a safety alert to be applied. A safety alert must be reviewed when: - the MSP is due to end: ○ An extended or replaced MSP will not retain a safety alert. It will need to be re-applied if appropriate - a significant change has occurred in a customer's circumstances or behaviour, such as: ○ a new incident of actual or attempted assault or actual stalking occurs that results in the need to apply different service restrictions For a long-term MSP, a safety alert approved decision maker should consider recommendations from a LAP or ZAP to help inform their decision. To Record and approve the safety alert review outcome see Table 3
14	**Consider Notification Alert status** + Read more ... Check if the customer has an active Notification Alert: - A Notification Alert will not carry over to a new MSP if extending or replacing an MSP and will need to be re-triggered if still required - The customer image will carry over to a new MSP and remain on the s47E(d) tab if extending or reviewing the MSP with the Notification Alert - To remove the s 47FE(d) file/s: ○ Manager or Delegate level CIMS access is required. See Accessing and using the Customer Incident Management System (CIMS) for more information ○ see Table 3 in Notification Alert
15	**Consider Personalised Services referral** + Read more ... Consider if a referral to Personalised Services is appropriate. Referrals to PS from all other areas are assessed to decide on their suitability for PS case management. The reasons for referral are: - customer aggression - counterproductive behaviour - complexity - vulnerability - significant privacy breach - highly sensitive issues, such as involving the media or a high profile person - unreasonable or vexatious complaints **Examples of correct referrals** - The customer would benefit from a national, phone-based, case management service approach. - A serious incident has occurred with police involvement – make a referral immediately - The customer is not complying with a Managed Service Plan (MSP) - The customer uses unpredictable or aggressive behaviour - The customer makes a threat, real or implied, to local staff and Service Centre - recommendation specialist or professional has recommended it - The customer has had repeated incidents of counterproductive behaviour - There is a real and immediate threat of media or external escalation - The customer is experiencing vulnerability and risk issues, such as being transient or having a history of being incarcerated

	CIMS includes a Referral to Personalised Services strategy with the following referral drop down options: • Behavioural • Complexity • Privacy Breach • Sensitivity • Vexatious • Vulnerability Personalised Services will assess and determine the suitability of the customer. **Note**: If a customer is already managed by Personalised Services and the review outcome is for the customer to remain in PS, code the referral as part of the MSP review workflow. See Referring customers to and handling customer enquiries and correspondence for Personalised Services. See Table 2.
16	**Shared premises joint MSPs with service channel restrictions** + Read more ... If a mutual customer involved in an incident has a joint MSP in place, Services Australia and partner agency staff conduct the MSP review as part of a Local Assessment Panel (LAP) or Zone Assessment Panel (ZAP). Restricting face to face servicing to a premises needs agreement from the premises holder. Consideration will be given to the method of informing the customer of the servicing outcome. If agreed, Services Australia may relay the advice by telephone or SMS with a supporting letter. Include the following information when communicating with the customer by phone or in writing: • details about future servicing and the agreed access channels to partner agency services available on site, such as NDIA, ATO or DVA • an explanation of how the customer can contact each agency's OMC/PSSO, if the other agencies appointed one • if the partner agency intends to implement or extend a service channel restriction while Services Australia does not, there will be no restriction of access to premises where Services Australia is the premises leaseholder • the position titles of each agency's representative, for example: "Manager, <PLACE> Service Centre and Manager, <PLACE> NDIA" Both Services Australia and the partner agency should retain a copy of the MSP outcome letter. Services Australia and the partner agency staff must record any outcome impacting service on their approved customer management system/record. The relevant CANOC, CAPT and Face to Face Partnerships team can be contacted for support and advice. See Resources for a link to the Protocol Agreement Between Services Australia and Partner Agencies.
17	**Transfer of an MSP customer to a new Service Zone (Centrelink customers only)** + Read more ... A zone transfer of a current MSP customer occurs when there is a permanent change to their residential address to a different zone. See Table 3 in Customer service delivered through a One Main Contact (OMC) as part of a MSP.

Record the review outcome and notify the customer

For Shared Premises customers, if a joint MSP is in place or Services Australia has restricted the customer from attending its premises, partner agency staff must record any outcome impacting their service on their approved customer management system/record.

Table 2: how staff record and approve an MSP review and notify the customer of the outcome.

Step	Action
1	**Record the MSP review recommendation note and notify stakeholders** + Read more ... Record the MSP review recommendation note in CIMS. This note type is mandatory for MSP reviews. If the outcome is to extend or replace the MSP, the note will automatically transfer over to the new MSP.

	Find the MSP to be reviewed, using either: • the link in the reminder email, if there was one • the s47E(d) option in the customer's record Add a recommendation note to the MSP. s 47E(d) • Select s 47FE(d) and enter the note. This note will support the **Rationale for Decision** in the new MSP. Include the following: ○ a summary of the LAP or ZAP meeting ○ OMC or PSSO recommendations that have been accepted or rejected ○ the status of any servicing strategy that has not been completed by the end of the MSP s 47FE(d)
2	**Record MSP proposal** + Read more ... To start a review, s 47FE(d) • • • • **Update servicing strategies** Update the mandatory strategy to review and update MSP details in CDMS/CUBA. All servicing strategies recorded in CIMS start with a status of 'Not Started' and must be updated to reflect the progress of the strategy. The available servicing strategy progress updates are: • Not required: ○ in mandatory strategies, this is used when a customer is not a shared customer of the other service brand, or when the MSP was implemented prior to 1 July 2022 ○ in non-mandatory strategies, this outcome confirms that the strategy no longer suits the customer's circumstances • In progress - confirms the item is in progress and requires ongoing attention • Completed - used when the strategy has been completed throughout the period of the MSP. For mandatory strategies, completed reflects that the customer is a shared customer of the other service brand and the core system has been updated with the MSP details When an MSP applies to more than one service brand, make sure the relevant systems (CDMS or CUBA) are updated with the review outcome and MSP End Date. Notify the HSDD CANOC or Child Support PSSO of the decision and request the update of CDMS or CUBA if required. If Personalised Services (PS) is managing the administration of a directly referred proactive MSP, PS informs the relevant CANOC before processing in CIMS. See Resources for the CAPT networks and stakeholders contact list. For more information about direct referrals see: • Referring customers to and handling customer enquiries and correspondence for Personalised Services • Managed Service Plan (MSP) - Proposing, recording and approving If the outcome of the review is to: • extend or replace the MSP, go to Step 3 • end the MSP on approval or its original end date, go to Step 4

3	**Extended or replaced MSPs** + Read more ... Extending or replacing an MSP makes a new MSP record in CIMS. The record will have a new MSP ID. CIMS will automatically complete all of the following, using the content of the existing MSP. • Zone • Customer • Start date this will be the day after the existing MSP ends • Channel Restrictions all of these will have a draft status • Review recommendation notes included in the previous MSP • Link to the previous MSP • Mandatory servicing strategies • Employee responsible • Employee recording the MSP • One Main Contact/PSO • Backup OMC • Restriction Approver Check all of the above, and update them if necessary. Use the same process as recording a new MSP See Managed Service Plan (MSP) Proposing, recording, and approving. Does a safety alert need to be applied? • **Yes**, go to Table 3 > Step 3 • **No**, go to Step 5.
4	**Exit to mainstream on approval or end date** + Read more ... For an exit to mainstream on approval, the MSP will end at 11:59pm on the day that the proposal is approved. For an exit to mainstream on end date, the MSP ends at 11.59pm on its original end date.
5	**Rationale for decision note** + Read more ... All MSPs must include a **Rationale for decision** note. Use the s47E(d) button to create this note. As a minimum, the note must contain: • a rationale for the length of the MSP • a brief summary of the behaviours or vulnerabilities that led to recommending, extending or replacing an MSP • a description of the vulnerabilities the customer is experiencing, and how the servicing strategies aim to address these • an expected completion date for each servicing strategy • a description of the ongoing risk the customer poses to staff in each service brand • the reasons for deciding on the OMC/PSSOs chosen to support the customer All free text notes recorded in an MSP are subject to Freedom of Information (FOI) Act provisions. See Freedom of Information (FOI) for further information. See Resources page in Accessing and using the Customer Incident Management System (CIMS) for MSP notes and examples, including the rationale for decision.
6	**Draft MSP Review Outcome letter** + Read more ... Draft the MSP Review Outcome letter. See Resources for the letter template. The MSP must have a draft letter attached before submitting it for approval. The letter must: • describe the behaviour of the customer when relevant • describe any relevant considerations taken into account in making the decision • explain the customer's ongoing access to Services Australia's services • outline the customer's right to request a review of the MSP

	Note: in the letter do **not** use exact (verbatim) quotes of what the customer said. For help, contact Customer Aggression Prevention Team (CAPT) before issuing the letter. Attach the draft to the MSP.
7	**Submit the reviewed MSP for approval** + Read more ... Select s 47FE(d) . This sends the proposal to the Review or Restriction approver, and Personalised Services. CIMS will show an error message if a mandatory field still needs to be completed. Select the error message to open the error in full.
8	**Approve, reject, or send back an MSP** + Read more ... CIMS automatically emails the approver when the recommendation is ready to review. The reviewer should now read through the recommendation and decide between the following 3 choices: • approve the review • send it back to the submitter for changes • reject the review If call customisation is included as a servicing strategy, this should form part of the MSP approval process. For details about call customisation implementation, see Table 1 in Managed Service Plan (MSP) Proposing, recording and approving. If an email redirection is included as a servicing strategy, this should also form part of the MSP approval process. **Approve the MSP review** + Read more ... s 47FE(d) **Reject or send back the MSP review** + Read more ... s 47FE(d)
9	**Advise the customer of the decision** + Read more ... The OMC should call the customer (before they receive the letter) to advise the outcome of the review. Document details of discussion: In the MSP record a **Customer Contact Outcome** note. The note should include the following details: • Contact reason: (Commencement of MSP) • Time: • Discussion: • Behaviour and warnings: • Updates to record: **Write to the customer and attach the letter to the MSP** Advise the customer in writing to tell them the outcome of the review, even if there is no change to the MSP. If Personalised Services is managing this customer, the PSSO will contact them to tell them the outcome. **Send an SMS notification** Only an approved decision maker can decide whether to send an SMS. **Note:** Use judgement when making the decision to contact a customer via SMS to advise of the MSP review outcome.

	See Sending a Desktop Electronic message to a customer and the DEMC messages user guide. An SMS does not contain all of the required notification and decision information. The SMS does not replace the corresponding letter. **Send a letter** Send the approved MSP letter. Include the OMC/PSSO contact card. The MSP letter delivery method is determined by service restrictions on the MSP. See Managed Service Plan (MSP) - Implementing for more information. In some serious cases, police may hand the letter to the customer. If this occurs, it **must** be recorded in the MSP. The MSP letter should still be delivered according to the relevant method. Attendance at a service centre in non compliance with the servicing restriction may be an offence under the relevant trespass laws and actions may be taken should attendance occur. As such, delivery of these letters must meet the legal definition of 'service' and proof of delivery confirmed to progress legal action. Make sure that only the final approved letter, n PDF format, is attached to the MSP. Staff or security guards must not leave the premises to hand the letter to the customer. In some serious cases, the letter may be hand delivered by the local police (where these arrangements exist). Record this in the MSP notes. See Resources for the MSP letter guidelines, including information about postage and delivery and a links to the Ordering business cards, employee contact cards page. For more information about implementing MSPs, see Managed Service Plan (MSP) - Implementing.

Record and approve the safety alert review outcome

Table 3

Step	Action
1	**Who can record a safety alert review outcome for Centrelink customers** + Read more ... Where a review of a safety alert has been completed and the decision is to reapply, a new safety alert **must** be proposed and approved. • Staff with CIMS Manager and Delegate access can propose a safety alert • CIMS Delegate can record the review outcome as the approved decision maker, or on behalf of the approved decision maker. • For each safety alert decision, a Safety Alert Decision note is required **Note:** MSPs and safety alert information can be released under the Freedom of Information Act. All information in CIMS must be factual, use exact quotes (verbatim), and cannot include personal commentary or opinion.
2	**Safety alert decision maker** + Read more ... The inclusion of a safety alert review is a component of the MSP review approval process. The person responsible for a safety alert is the same decision maker for MSPs. See MSP decision making table.
3	**Recording and approving the safety alert outcome** + Read more ... If the safety alert review decision is to cease, go to Step 4 **Extend or Replace safety alert** The Extend MSP and Replace MSP review functions will not carry across the safety alert from the existing record. A safety alert entry will need to be created for the approved decision maker to consider in the new MSP. To reapply a safety alert: s 47FE(d)

	s 47FE(d) **Note:** after a safety alert has been saved or submitted, notes saved to the MSP s47E(d) cannot be edited. See Managed Service Plan Proposing, recording and approving for how to ask for removal of an incorrect note s 47FE(d) Where the staff member recording the safety alert review outcome is the restriction approver or is processing the decision on their behalf: s 47FE(d) See Resources page in Accessing and using the Customer Incident Management System (CIMS) for MSP notes and examples, including the rationale for decision
4	**Ceasing the safety alert and the MSP** + Read more ... Is the review decision to cease **both** the safety alert and the MSP? • **Yes**, the safety alert will automatically end when the MSP ends. Create appropriate Safety Alert decision note (approve). See Managed Service Plan – Proposing, recording and approving for minimum requirements and examples • **No**, go to step 5
5	**Cease safety alert only** + Read more ... • For staff with CIMS Manager or Delegate access: s 47FE(d) After a safety alert has been saved or submitted, notes saved to the MSP s47E(d) cannot be edited. See Managed Service Plan – Proposing, recording and approving for how to ask for removal of an incorrect note s 47FE(d) Where the staff member ceasing the safety alert is the restriction approver or is processing the decision on their behalf: s 47FE(d)

Resources

s 47FE(d)

MSP letter templates and guidelines

Letters sub site General Correspondence

See:

- Guide to MSP and Warning letters templates
- Medicare Provider Warning
- MSP Face to face call restriction direct to another location
- MSP Invitation to Participate in Review
- MSP One off variation of restriction
- MSP Proactive
- MSP Provisional
- MSP reminder of face to face call restriction direct to another location
- MSP Reminder of write only
- MSP Review Outcome
- MSP Write only
- Warning Behaviour

MSP SMS Guide

Centrelink letters online and Desktop Electronic Messaging Capability (DEMC) messaging user guide

Contact details

Customer Aggression Prevention Team (CAPT)

Customer aggression prevention - networks and stakeholders

Service channel restrictions

See Managed Service Plan (MSP) - Proposing, recording and approving for information on full and partial service channel restrictions.

Customer Incident Management System (CIMS)

Customer Incident Management System

Intranet links

Adverse Customer Event Response

Agents and Access Points

Customer Aggression Prevention Hub

Customer aggression prevention - networks and stakeholders - list of contacts

Customer aggression A - Z

OMC/PSSO contact cards, Ordering business cards, employee contact cards, name badges and desk plates

Intervention, Protection Orders and Apprehended Violence Orders in Australia

Managed Service Plan (MSP) - Customer not complying

Legal Services Division

Protocol Agreement Between Services Australia and Partner Agencies

Security Hub

Service Centre Security

Staff support and employee assistance

Health and Wellbeing Hub

Health and Safety

Ministerial delegations and authorisations (including Public Order (Protection of Persons and Property) Act 1971 (POPPPA))

Shared premises safety   WHS considerations

Services Australia website

Service commitments

Your responsibilities

Payment and Service Finder

s 22 s 22

s 47FE(d)

Australian Government

Services Australia

Customer aggression - Prevention and management 104-07000000

Currently published version valid from 6/10/2025 4:00 PM

Background

s 22

s 47FE(d)

This document provides staff with information and resources to guide the prevention and management of customer aggression and counterproductive behaviour.

Preventing and managing customer aggression

The Preventing and Managing Customer Aggression Policy establishes the framework for preventing and managing customer aggression and counterproductive behaviour. The Resources page contains a link to the policy.

Services Australia's approach focuses on:

- providing a physically safe and secure working environment
- well-prepared and skilled staff
- staff health, mental health and wellbeing
- effective management of aggressive customers
- implementing administration strategies to tailor the way services are delivered to customers, including providing internal referrals, for example, to social workers and other specialist staff

Managing incidents of customer aggression includes:

- in the face-to-face environment:
    - directing customers to leave the agency's premises under the Public Order (Protection of Persons and Property) Act 1971 (POPPPA)
    - a customer who is directed to leave may have face-to-face service restrictions. The agency defines trespass as ‘entering a person’s land without permission or remaining on a person’s land after being directed to leave’
    - customers not complying with a face-to-face restriction who have received advice that their implied licence to enter the premises has been revoked via a Managed Service Plan (MSP) letter, may be prosecuted for criminal trespass under s12 of the Public Order (Protection of Persons and Property) Act 1971 (POPPPA)
- communicating with police
- in the phone environment where a customer persists with aggressive or counterproductive behaviour:
    - managing the call in line with telephone standards procedure
    - escalating concerns of self-harm or threats to others
    - implementing call customisation s 47E(d)

    - applying emergency response procedures
- in the digital and written environment, conducting post-incident follow-up, including in very limited circumstances, implementing an email redirection (where the customer's communication is persistently threatening, harassing, or could cause harm or distress to the recipients)
- referral to a social worker when a customer:
    - is extremely distressed, or
    - indicates they are, or
    - have recently contemplated attempting suicide or self harm, or
    - has a general social worker enquiry
- after incidents of aggression, calling the customer to discuss behavioural expectations and identify any support needed. This may include issuing a letter to warn the customer of possible service restrictions where the behaviour reoccurs
- implementing Managed Service Plans (MSPs) for customers who place staff and other customers at risk. MSPs can limit or deny a person's access to our offices for a period. Service channel restrictions are considered agency wide. By restricting access, we limit the risk to our staff and other customers while continuing to support customers to receive access to their payments. During this period, a one main contact is implemented to contain the risk, proactively resolve triggers for aggression and focus on transitioning the customer to mainstream servicing. A One Main Contact (OMC) can make referrals to Personalised Services, and/or to social work services and other specialised business areas as needed
- applying a safety alert. This feature alerts staff to customers who have a history of incidents with a behaviour type of actual or attempted assault or actual stalking. Where there is **verified information** indicating a potentially high risk of assault occurring to agency staff, use discretion to apply a safety alert. For example, where the customer in known to carry a weapon or a serious assault by a mutual customer occurs. An active safety alert supports staff decision making for customer management and service centre response.
- applying a Notification Alert. This is a feature of an MSP that alerts staff in near real time to MSP customers who have had a recent incident recorded in the Customer Incident Management System (CIMS) that has the potential to significantly impact the agency's business or operations, for example incidents with a behaviour type of actual or attempted assault. For more information on Tier 1 and 2 escalations, see the Incident Management and Escalation Policy
- where a customer is not complying with the MSP arrangement, conducting an MSP review
- conducting Post Incident Reviews of serious incidents to mitigate the risk of further incidents

Legal avenues Service Australia can take to minimise the risk to staff and others include:

- liaising with police and prosecution regarding criminal charges, and
- obtaining, or assisting staff to obtain, protection orders that protect workplaces (available in the ACT and Tasmania) or individual staff (available in all states and territories)

Risk management

A planned and systematic process of managing risk that conforms to Services Australia's Security Risk Management Framework and Work health and safety (WHS) hazard and risk management. This includes:

- identifying any threats/opportunities arising from a person's behaviour or circumstances
- evaluating the threat
- implementing risk controls
- monitoring for any changes in threats/opportunities or a breakdown in the mitigation strategy
- monitoring Services Australia's external risk environment for any changes that may impact the nature or level of risk
- consulting with workers and their representatives
- consulting, co-operating and co-ordinating activities with other duty holders

Shared Premises with partner agencies, a combined approach

Some Services Australia sites share premises with other service providers including other Commonwealth departments and agencies, state government agencies, local government and private sector agencies and charities.

Each provider has duties under the Work Health and Safety Act 2011 to ensure workers in shared premises are (as far as is reasonably practicable), safe. As the leaseholder, Services Australia is responsible for providing a safe work environment.

The shared premises customer management protocol includes processes for Services Australia and partner agencies to manage and respond to incidents of customer aggression for all staff located within Services Australia service centres.

Aggressive Behaviour Response Model (ABRM)

Services Australia's approach to the management of customer aggression based on a zero tolerance for violence and a focus on staff and customer health, safety and security.

The model includes an approach of:

- de escalation when a customer is demonstrating counterproductive behaviour by modelling signs of calm behaviour, active listening, respect and empathy
- disengagement if a customer's behaviour escalates further, or if a staff member feels unsafe, by ceasing the interaction and seeking immediate support, including phone emergency response
- Emergency Response if the customer's behaviour becomes violent, including serious threats, by activating the duress alarm, moving to safety, calling the police, evacuating as defined in customer facing and non customer facing Emergency Response Procedures Aggression etc.

ABRM is Service Australia's approach to the management of customer aggression. Based on a zero tolerance for violence and a focus on staff and customer health, safety and security. The ABRM includes a focus on de escalation, disengagement when people feel unsafe, and an emergency response when a customer is violent or staff safety is at risk.

An interaction may move through different stages in a non linear way and escalate at any time. By modelling good listening skills, calm behaviour, active listening, and showing respect and empathy, we can often return a customer's behaviour to respectful and cooperative. De escalation skills are an important part of improving safety. The model is also clear that if a staff member feels unsafe, they should disengage, cease the interaction and seek leadership support.

If a customer's behaviour becomes violent, including threatened violence or where a customer talks about suicide/self harm, this requires an emergency response.

Incidents involving children

There is a zero tolerance of harm to children. If a staff member, in the course of their duties observes behaviour, which raises concerns about a child's safety, immediate action is needed. See Risk identification and management or threats to safety or welfare of a child.

Contact from customers through non-official digital channels

In situations where a customer contacts a staff member through non-official digital channels, for example, a staff member's personal social media account, it is generally open to the staff member to decide on their response, this includes:

s 47E(d)

The staff member should report such conduct to their manager. A written record of the conversation between the staff member and the manager should be kept. This is particularly important if the conduct has made the staff member feel unsafe.

If the staff member has concerns about their safety and they had a discussion with their manager about it, the conduct should be recorded in the relevant system. See Reporting, recording and escalating incidents of customer aggression.

The Resources page contains links to the Customer Aggression Prevention intranet page, intranet links and a link to the agency's Service Commitments on the Services Australia website.

Contents

Related links

Customers talking about suicide or self-harm

Family and domestic violence

Identifying customer vulnerability and risk issues

Interpreter Services for customers who are deaf or hard of hearing

Managing complaints and feedback

Providing services to customers with disabilities

Reporting, recording and escalating incidents of customer aggression

Risk identification and management of threats to the safety or welfare of a child

Referral to a social worker

Using National Relay Service (NRS)

Notification Alert

Process

s 47E(d)

This document provides staff with information and resources to guide the prevention and management of customer aggression and counterproductive behaviour.

Positively influencing customer behaviour

This table contains information about implementing customer service approaches that prevent or reduce the risk of customer aggression and counterproductive behaviour.

Title	Description
Vulnerable customers	**Consider factors impacting customers experiencing vulnerability** + Read more ... External factors, such as long wait times, poor service delivery or lack of available information may influence customer behaviours. The service we provide can rebuild the customer's relationship with Services Australia. Vulnerability may be identified through customer disclosure, customer cues or file review. Apply a sensitive approach to recognising difficulties customers may be facing based on their circumstances. Circumstances that may indicate a risk or, or experience of vulnerability include: • Safety concerns • Health concerns (physical, mental, disability) • Financial hardship • Housing • Experiencing a crisis or trauma • Limited support or connection Developing a risk-based approach to supporting customers experiencing vulnerability, inadequate coping skills and illness by being prepared to offer referrals to available resources, external service providers or agency specialist staff. This can help prevent and de-escalate customer aggression. Consider referrals to address any identified special needs of the customer: • Social worker • Indigenous Service Officer (ISO) • The Financial Information Service (FIS) Officer • Multicultural Service Officer (MSO) • Language Services (for example, translation of customer aggression letters) • Specialised and Intensive Services (SIS)

	• [Incarcerated Customer Services](#) • Job Capacity Assessment (JCA) Referral • Employment Services Assessment (ESAt) Referral • Community Engagement Officer (CEO) • Farm Household Case Officer (FHCO) • Aged Care Specialist Officers (ACSOs) • Grandparent, Foster and Kinship Carer Advisers • Personalised Services (PS) For more information about: • customers experiencing vulnerability see social work services • identifying customer vulnerability and risk issues, see Identifying customer vulnerability and risk issues • options for addressing potential barriers for Indigenous customers, (for example, remoteness and lack of access to mainstream services), see Identifying barriers to participation for Indigenous customers • identification and eligibility for Income Management see Identifying and assisting income managed customers • appointing nominees, their obligations, privacy issues and how to cease the arrangement see Nominees • external agencies, see External specialists/services • urgent claim processing, see Immediate new claim and non new claim priority processing • Local Peer Support (LPS), see Tier 0 technical support self sufficiency
Providing services to customers with disabilities	**Customers with a disability or medical condition** + Read more ... Many customers with a disability or medical condition face barriers and challenges in life. Being aware of a customer's disability and being able to understand how medical conditions can affect them helps in providing appropriate assistance. Service Officers should be aware of the impact of disabilities and medical conditions. For example, for customers who: • have a mental health condition, • have an acquired brain impairment, • are deaf, have hearing loss, or have a speech disability See Providing services to customers with disabilities.
Risk identification and management of threats to the safety or welfare of a child	**Incidents involving children** + Read more ... See Risk identification and management or threats to safety or welfare of a child.
Customers who may be experiencing family and domestic violence	**Assisting customers experiencing family and domestic violence** + Read more ... Through the implementation of Service Australia's Family and Domestic Violence Strategy, in particular the Family and Domestic Violence Support Model, the agency is able to identify at risk customers early and offer information, resources and support across all areas of the agency. The Resources page contains a link to the Family and Domestic Violence Support Model. See also: • Family and domestic violence • Customer referral guidelines for Child Support staff • Immediate new claim and non-new claim priority processing
Unfavourable decision	**Communicating unfavourable decisions** + Read more ... It is important to make genuine attempts to contact a customer to give them the chance to understand the decision and provide new information or evidence where appropriate. Clearly explaining a decision can prevent rework through complaints, reviews and appeals or objections, and repeat contact from the customer. It also gives the agency the chance to correct simple errors.

	Explaining decisions can help prevent or de escalate incidents by respectfully considering the customer's views and, if appropriate, quick referrals or follow up. When preparing to advise a customer of a decision about their payment or claim: • Have a clear understanding of the relevant policy or legislation; this enables you to explain the reason(s) for the decision in a confident manner • Make sure any commitments are followed up • s 47E(d) • If the customer expresses dissatisfaction with the decision, acknowledge their point of view, for example: s 47E(d) Provide appropriate options: • Listen to their needs and provide referrals if appropriate • Discuss their review and appeal rights If the interaction escalates. See De escalation techniques below For more information see: • Centrelink ○ Advising verbally of an unfavourable decision (CLK) ○ SME quality checks, ARO referrals and implementing ARO decisions • Child Support ○ Contact with Child Support customers
Telephone standards	**Apply telephone standards** + Read more ... Service Australia's telephone standards provide further details on the process of de-escalation and disengagement - when to use a malicious call trace, end a call with a customer, or initiate an emergency response. For information about providing customer service over the phone, see: • Centrelink staff - Answering calls in Centrelink • Child Support staff - Contact with Child Support customers • Medicare staff – Telephone standards for Medicare and Health Delivery For more information about malicious call trace see the Table 2 in Customer aggression - Response See the Resources page for a link to the Services Australia Workspace Quick Reference Guide on the Intranet.
De-escalation techniques	**De-escalating the interaction** + Read more ... s 47E(d)

s 22	s 22 s 47E(d)
End phone call	**Ending/discontinuing customer phone calls** + Read more ... Sometimes de-escalation may not work. In such cases, end the call. s 47E(d) **Warn the customer before ending a call**

	Explain to the customer the call will be discontinued if their behaviour continues. Inform the customer that the agency expects its staff to be treated with respect and courtesy and it is difficult to help when a customer is not acting accordingly. **Example** 'I may not be able to continue this call with you because you are (quote behaviour). This is making it hard for me to help you. If you continue to (behaviour) I will end the call without any further warning and discuss this with my manager/team leader.' If the behaviour continues, inform the customer the call is ending. End the call politely.
Disengage	**Customer's behaviour escalates** + Read more ... If the customer's behaviour escalates further, or if a staff member feels unsafe, disengage. For Smart Centre staff, see Telephony standards procedures. Seek immediate leadership support in line with the Aggressive Behaviour Response Model (ABRM). The team leader/manager should make a decision about the response with consideration of personal safety and the safety of people in the site, and with awareness that disengaging may escalate aggressive behaviour. If the behaviour is aggressive, there is an intent to cause harm and/or the impact potentially endangers the safety of staff and others, this is a customer aggression incident and the response should be to disengage, and/or initiate an emergency response. For more information, see Customer aggression - Response. Service Australia may implement an MSP to tailor how we deliver services as a strategy to improve the safety of staff, the public and agency property. MSPs can include a full or partial restriction to a customer's access to one or more service channels. For more information about responding to phone threats, see Customer aggression - Managed Service Plan (MSP).
Proactive Managed Service Plans (MSPs)	**Proactive MSPs** + Read more ... Proactive MSPs provide a support mechanism for customers with barriers or vulnerabilities rather than as a response to an incident. A proactive MSP can act as a preventative strategy for customers who may be a threat to staff safety. Service Australia may implement a proactive MSP to tailor the delivery of services to customers with identified vulnerabilities, barriers, aggressive or counterproductive behaviours. A proactive MSP may or may not include service restrictions depending on the circumstances of the case, for example: • No service channel restrictions: ◦ To support a homeless customer with health issues while they navigate the process to apply for the Disability Support pension • With service channel restrictions: ◦ To maintain staff safety based on the service officer in Face to Face Incarcerated Customer Servicing team advise that a prison release customer may pose a risk to staff safety See Customer aggression - Managed Service Plan (MSP) for further detail about MSPs and for details of the relevant Customer Aggression Network Operational Contact (CANOC). **Smart Centres (including Assessment Services Branch)** Smart Centre Team Leaders and Managers should discuss MSP referrals with the Smart Centre Customer Portfolio Operations team who are responsible for submitting MSP recommendations to the relevant Zone CANOC. If a Smart Centre Team Leader or Manager needs to contact the Smart Centre Customer Portfolio Operations team, they should email Smart Centre Escalations. **All other business areas**

	Contact the relevant Zone CANOC for further advice. **Service Delivery Partners MSP referrals** If a Service Delivery Partner thinks an MSP is needed a Team Leader or Manager of that site should email the Smart Centre Customer Portfolio Operations team, they will liaise with the relevant Zone CANOC. If a business area needs to contact a service delivery partner about a customer or to discuss an MSP they should email Smart Centre Escalations **Shared Premises** If an incident occurs with a partner agency or a mutual customer in a shared premises, both Services Australia and the partner agency collaborate on an agreed response. This may include a joint agreement to implement service channel restrictions to premises and services. This may result in a different servicing outcome for each agency. For assistance, contact the relevant Zone CANOC. For more information, see Customer aggression Managed Service Plan (MSP).
Seek further assistance	**Assistance** + Read more ... **Your manager** - Providing debriefing and support after an incident of aggression is a key role of Service Australia managers. The responsibilities of managers includes following the procedures outlined in the Emergency Response Procedures**.** **Regional Security Advisors (RSAs)** - RSAs are staff who work in the Security Branch and give security advice and support for staff. This includes: • immediate advice in response to a security incident • obtaining an image of the customer from the CCTV footage to attach to the Notification Alert • liaising with the police • undertaking Security Control Reviews • participating in Post Incident Reviews **Emergencies** - in the event of an emergency, call 000. **CANOCs** are subject matter experts in the prevention and management of customer aggression and they can help record and respond to incidents of aggression. Contact the local Customer Aggression Network - Operational Contacts (CANOC) **Customer Aggression Prevention Team (CAPT)** via email.
Feedback	**Providing feedback** + Read more ... The Customer Aggression Prevention Team (CAPT) encourages staff feedback about the prevention and management of customer aggression and counterproductive behaviour. To provide feedback about Operational Blueprint files use the Feedback link in the top right corner of the page. Where a One Main Contact (OMC) or Personalised Services Service Officer (PSSO) becomes aware that a customer they are managing has been served outside of the servicing arrangements, contact the local Customer Aggression Network - Operational Contacts (CANOC).

References

Legislation

Links to the Federal Register of Legislation site go to an 'All versions' page. Select the 'Latest' version.

Age Discrimination Act 2004

Australian Human Rights Commission Act 1986

Disability Discrimination Act 1992

Human Services (Medicare) Act 1973

Ombudsman Act 1976

Privacy Act 1988

Public Governance, Performance and Accountability Act 2013

Public Order (Protection of Persons and Property) Act 1971 (POPPPA)

Racial Discrimination Act 1975

Sex Discrimination Act 1984

Social Security (Administration) Act 1999

Work Health and Safety Act 2011

Resources

Contact details

Customer Aggression Prevention Team (CAPT)

Scroll down the Customer Aggression Prevention - Networks and Stakeholders page for Customer Aggression Network - Operational Contacts (CANOC) and Customer Aggression Network (CAN) contact details.

Services Australia Security Hotline

Roles and responsibilities - Customer aggression management

This table defines the staff and team roles and responsibilities when incidents of customer aggression occur.

Team/Staff	**Responsibility**
Aggression Response Team (ART)	Staff responsible for coordinating the site's response to incidents of customer aggression. Listed in each site's Emergency Response Procedures - Aggression (ERPAs).
Customer Aggression Network (CAN)	Leadership representatives, who meet monthly to share information on best practice, drive consistency and ensure compliance with procedures. They contribute to mitigating the risk of customer aggression in their workplace by coordinating Zone Panels and providing staff support. Contact details for CAN
Customer Aggression Network-Operational Contact (CANOC)	Senior subject matter experts who work on the management and coordination of customer aggression incidents. They work collaboratively with stakeholders to support the effective application and continuous improvement of Services Australia's Customer Aggression Prevention and Management policy and procedures. Contact details for CANOC
Customer Aggression Prevention Team (CAPT)	A team within the agency that provides program management advice for the prevention of customer aggression. Their focus is on helping staff and Services Australia prepare for, respond to, recover from and prevent customer aggression. Contact details for CAPT
Incident Leadership Contact	Person responsible for management of the incident, including actioning activities relating to a Managed Service Plan (MSP). Physical security may contact this person.
Local Assessment Panel (LAP)	A group of local leaders within a site or region who meet to discuss aggression incidents. A decision is made to determine the best customer management approach, including support options and service restrictions.

	For structure details of Local Assessment Panels (LAPs), see Local Assessment Panels (LAPs) table.
One Main Contact (OMC)	An appointed contact for a customer. Defined within a Managed Service Plan (MSP) and responsible for managing the customer's interactions with Service Australia.
Personalised Services Service Officer (PSSO)	A Service Officer from the Personalised Services team who is case managing the customer as defined within a MSP (CLK and CS only). Personalised Services.
Regional Security Advisor (RSA)	Staff who work in the Security Branch and provide security advice and support for staff, including immediate advice in response to a security incident, obtaining an image of the customer from the CCTV footage to attach to the Notification Alert, liaising with the police and post incident reviews.
Security Guard	A person engaged to enhance the safety and security of employees, customers and visitors as well as assets.
Staff roles	Customer Aggression - Managed Service Plan (MSP), letter and SMS decision makers
Zone Assessment Panel (ZAP)	A group of local leaders within a Zone who: • meet to discuss aggression incidents • decide the best customer management approach, including support options and service restrictions • develop or review MSPs including any Notification Alerts active at the time of review They give coordination and a consistent approach to complex customer management and help proactively manage customer aggression risks. For structure details of Zone Assessment Panels (ZAPs), see Zone Assessment Panels (ZAPs) table.

Family and Domestic Violence Support Model

s 22

Family and Domestic Violence Support Model

Intranet links

Our approach to aggression - to see Preventing and Managing Customer Aggression policy

Emergency Response Procedures - Aggression (ERPAS). For sites providing face to face services

Incident management and escalation policy

Work health and safety (WHS) hazard and risk management

Reporting and recording workplace health and safety (WHS) incidents

Legal Issues - Customer Aggression

Personal security

Working Away from the Office

Customer Aggression Network - Operational Contact (CANOC) role

Customer Incident Management System

Service Zone Support Centre

Health and Safety

Security Incident Reporting

Employee assistance program

Services Australia website

Service commitments

Your responsibilities

Payment and Service Finder.

External websites

Commonwealth Ombudsman better practice guides, see:

- Better practice guide to complaint handling
- Better practice guide to managing unreasonable complainant conduct

Ombudsman New South Wales   Complaints handling resources

Training & Support

The agency's customer aggression training, the Managing Aggressive Behaviour Program (MAB Program) is mandatory for customer-contact staff and their direct supervisors.

Customer aggression prevention training further supports staff with ‘Learning Bites’ about preventing and managing customer aggression. ‘The 4 WHYS to record’ provides information to promote when and where staff record incidents of aggression and counterproductive behaviour. All customer aggression prevention Learning Bites and staff resources can be found by navigating to the relevant topic on the Customer Aggression Prevention Hub.

The Customer Aggression Training Summary outlines role required and recommended learning for; service delivery staff and their direct supervisors, staff who record, review and/or approve Managed Service Plans (MSPs).

CIMS role required learning is for all Centrelink service delivery staff and their direct supervisors. It is also role required for staff who record, review and/or approve Managed Service Plans (MSPs).

Australian Government

Services Australia

Customer aggression - Response 104-07020000

Currently published version valid from 18/11/2025 8:11 PM

Background

s 22

s 47FE(d)

This document explains how staff respond to threats, customer aggression and counterproductive behaviour. It also includes instructions for coordinating a response to an emergency.

Emergency Response Procedures - Aggression (ERPAs)

The Emergency Response Procedures - Aggression (ERPAs) include:

- instructions for staff responsible for coordinating an emergency response
- the assigned responsibilities, actions and equipment required in the event of an emergency specifically relating to aggression incidents. This could be an event that requires a significant and coordinated response

ERPAs complement the site's Emergency Response Procedures for other emergencies to which the site may need to respond. Such as:

- fire
- chemical
- bomb threats
- medical emergencies

Site leaders:

- should implement ERPAs in combination with customer aggression training
- must communicate the ERPAs to staff
- give all staff a Quick Reference Guide. The guide must include key information about their role and responsibilities when responding to aggression

Aggression Response Team (ART)

The ART is a group of specified senior staff at a site who have defined responsibilities for responding to customer aggression incidents. The ART will include:

- the manager
- team leaders

Other ART members may also include:

- social worker
- job capacity assessor
- chief warden
- health and safety representative
- first aid officer

If the site is a shared premises, the ART should include representatives from co located agencies. The ART members are listed in the site's Emergency Response Procedures Aggression (ERPAs), under the key contacts heading.

When ART members are offsite or on leave, they should:

- arrange for backup staff to take on their responsibilities
- communicate the backup arrangement to all staff

During an incident, the ART will:

- respond when staff activate a duress alarm. Any staff member can activate a duress alarm to alert others and get support in the event of aggression
- assess whether staff or other people are at risk of injury (including self harm)
- decide if staff or other customers should move away from the person or incident
- consider whether support is required from police, fire or ambulance
- initiate a s47E(d) , including evacuating the immediate area or site
- coordinate first aid for staff or others
- give instructions to staff on site

See the Resources page for links to Workplace emergency management and Workplace emergencies - Human-caused hazards or emergencies.

Aggressive Behaviour Response Model (ABRM)

The Aggressive Behaviour Response Model describes how the agency responds to customer aggression or counterproductive behaviour. It includes a focus on de-escalation, disengagement when people feel unsafe, and an emergency response when a customer is violent or staff and customer safety is at risk.

There are 4 stages of the ABRM:

- respectful interaction
- de-escalation
- disengagement
- emergency response

An interaction may move through different stages in any order. It can escalate at any time, depending on the type of behaviour and the response options available. Skipping stages or steps may be necessary to respond to a situation safely. Some incidents may be managed effectively in a single stage of the ABRM. All decisions should be made with consideration of personal safety and the safety of people in the site.

Violence and threats of violence require an emergency response. This response can include:

- using the duress alarm
- s47E(d)
- locking the customer entrance
- calling police or emergency services as appropriate
- adding a Notification Alert

Non-physical offensive conduct

Non-physical offensive conduct is behaviour that offends another person. This may include threats, offensive language, or intimidating communication or behaviour.

Staff must try to de-escalate this behaviour using the Aggressive Behaviour Response Model. Start by asking the customer to stop their behaviour. If the customer refuses, staff must tell them to leave the premises.

Responding to threats

Threats of harm can be made through any service or other channel. The threats can be:

- to staff
- other customers/members of the public
- property or environment

For threats made on the phone, see:

- the Process page for procedures in non customer facing sites
- the Resources page for the ERPAs for face to face staff including Contemporary Service Centres

Incidents involving infectious/communicable diseases

Deliberately coughing towards staff, spitting at the ground or towards staff and/or threatening staff with an item that is or could transmit infectious/communicable disease, for example a syringe, are all aggressive behaviours that threaten staff health and safety. They must be reported and recorded as a customer aggression incident in:

- Customer Incident Management System (CIMS) for Centrelink customers
- Customer Incident Recording Tool (CIRT) for Child Support or Medicare customers

Blood and other bodily fluids/substances can carry infectious and communicable diseases. Any person who uses them to threaten staff is engaging in unacceptable behaviour and staff should follow usual emergency response and decision making protocols.

If a staff member suspects they have been exposed to an infectious disease, follow the safe operating procedures for exposure to blood and other bodily fluids/substances, on the Infection Control page.

All suspected exposures to infectious/communicable diseases must be reported to your manager and an incident recorded in Our Safety.

For more information about infectious/communicable diseases see Resources page for links.

Locking the customer entrance in response to threat or incident

At times, a site will lock the site entrance rather than initiate a s47E(d) response. s47E(d)

In non-customer facing sites, a s47E(d) response is the same as a site closure. Staff and customer safety is the main priority when deciding to lock the entrance. See the Process page for more information.

s 47E(d)

Trespass

The agency defines trespass as ‘entering a person’s land without permission or remaining on a person’s land after being directed to leave’.

If, for example, the agency implements a face-to-face servicing restriction for a customer and issues the customer with an MSP letter, it revokes consent for the customer to enter an agency site for a period of time. Customers not complying with a face-to-face restriction may be prosecuted for criminal trespass under s 12 of the Public Order Act.

Directing a person to leave a site

Any staff member can ask a person to leave the premises.

Reasons for doing so include:

- a person’s behaviour makes it unsafe to keep serving them, such as:
  - escalating behaviour
  - verbal abuse
  - yelling
  - intimidation
  - threats of violence
- a person has damaged property or is threatening to do so
- people are arguing, fighting or being disruptive
- a person has assaulted another person

s 47E(d)

If a person refuses to leave the premises, an authorised staff member under the Public Order (Protection of Persons and Property) Act 1971 (POPPPA) can direct the customer to leave. The legislation makes it a criminal offence for a person to refuse or neglect, without reasonable excuse, to leave Australian Government premises upon being directed to do so by an authorised person (subsection 12(2)).

Scenarios where a direction can be issued include:

- a non violent demonstration at a site
- when a person refuses to leave a site after being asked to do so
- when a person attends a site in breach of their Managed Service Plan (MSP)

Only authorised staff can give the direction.

See the Resources page for links to the Public Order Act and Ministerial delegations and authorisations information.

If the person refuses to leave, call the police immediately. An emergency response may be necessary. A customer who refuses to leave is trespassing or failing to follow a lawful direction under the POPPPA. See Resources for links to the Emergency Response Procedures   Aggression (ERPA).

Security guards

Security guards may be deployed to service centres to help:

- protect people and assets
- prevent crime
- support incident management

s 47E(d)

See the Security Guard Guide for more details about guard's roles.

Managed Service Plans (MSP) with service channel restrictions

A customer may have a Managed Service Plan (MSP) in place. This is a way to tailor how services are delivered to the customer and can include restrictions on how they can contact the agency.

After an incident of customer aggression, consider an MSP to minimise any risk of customer aggression or counterproductive behaviour.

If a customer has an active MSP and does not comply with service channel restrictions, refer to Customer not complying with a Managed Service Plan (MSP).

Unreasonable complainant behaviour

Complainant behaviour becomes unreasonable when it goes beyond the usual behaviours customers display when they have a grievance or a dispute. It exceeds what a reasonable person would consider acceptable in the circumstances. Unreasonable behaviour hinders the agency’s ability to manage the customer's business and may obscure genuine issues. The Customer Complaints and Feedback Policy is available on the Process page in Managing complaints and feedback.

The Resources page contains links to:

- Emergency Response Procedures   Aggression (ERPA)
- infectious/communicable diseases
- phone bomb threat checklist
- Services Australia Workspace Quick Reference Guide
- Public Order (Protection of Persons and Property) Act (POPPPA)
- Services Australia Security Hotline
- Customer Aggression Prevention   Frequently asked questions
- other intranet pages

Contents

Psychological consultation service and referral process for forensic matters

Customer aggression   Reporting, recording and escalating incidents

Customer aggression   filming, recording and photography

Customer aggression   Post incident contact

Customer aggression   Escalating incidents

Notification Alert

Related links

Customer aggression - Prevention and management

Customer aggression - Staff support

Customer aggression - Managed Service Plan (MSP)

Managing complaints and feedback

Family and domestic violence

Customers talking about suicide or self-harm

Social work services

Process

s 47E(d)

This page has information on how to respond to threats, customer aggression and counterproductive behaviour.

On this page:

Aggression Response Team (ART) - Roles and responsibilities

Emergency responses to customer aggression

Responding to stalking and off-site harassment

Responding to virtual threats to harm staff or damage agency property

Responding to written threats to harm staff or agency property

[Making a decision to lock the entrance to a site in response to a threat or incident]

[Responding to incidents related to infectious and/or communicable diseases]

[Satisfaction Research Program Security incident notification and escalation process]

Aggression Response Team (ART) - Roles and responsibilities

Table 1: examples of the actions responders take to customer aggression.

Role	Responsibilities
First responder	**First responder actions** + Read more ... s 47E(d)
Second responder	**Second responder actions** + Read more ... s 47E(d)
Third and later responders	**Third and later responders' actions** + Read more ... s 47E(d)

Emergency responses to customer aggression

Table 2: examples of customer behaviour and suitable staff and site leadership responses for each stage of response.

Item	Description of customer behaviours, staff and site leadership response
1	**Customer attends in breach of MSP** + Read more ... Refer to Managed Service Plan (MSP) - Customer not complying, Process page Step 2. For customers with partial face to face services, see Step 3.
2	**De-escalate - face to face environment** + Read more ... Examples of customer behaviours include: • Raised voices between customers • Loud swearing • Agitated movements **Staff response** s 47E(d) For more information on de-escalation techniques, see De-escalation.
3	**Disengage - face to face environment** + Read more ... Examples of customer behaviours include: • Escalating behaviour

	• Intimidation through invasion of personal space • Violent gestures or threats of violence **Staff response** s 47E(d) See Disengage. s 47E(d)
4	**Duress - face to face environment** + Read more ... Examples of customer behaviours include: • Sustained loud swearing, verbal abuse or yelling • Customer coughing towards staff • Customer spitting at the ground or towards staff • Threatening staff with an item that is or could transmit infectious/communicable disease, for example a syringe • Intentional aggressive movements • Hostile or argumentative situation with staff or customers • Refusing to leave the site • Self-harming **Staff response** s 47E(d) **ART response** s 47E(d)
5	s47E(d) **- face to face environment** + Read more ... s47E(d) is the response to a severe threat where staff and other people are involved in a direct physical threat that could result in injury s 47E(d) s 47E(d)

	s 47E(d) Intentionally coughing or spitting toward staff or threatening to spit or infect others with a communicable disease. **Staff response** s 47E(d) **ART response** s 47E(d)
6	s47E(d) **- non-customer facing environment** + Read more ... In a non-customer facing environment, s 47E(d) • • • **Staff response** s 47E(d) **ART response** s 47E(d)
7	s47E(d) **- face to face environment** + Read more ... • s47E(d) is the response to an extreme threat level that could result in serious injury or death to customers and staff. s 47E(d) s 47E(d)

s 22	s 22
	s 47E(d) **Staff response** s 47E(d) **ART response** s 47E(d) Refer to the Resources page for a link to the Emergency Response Procedures - Aggression (ERPAs) including s47E(d) for a link to the Code Grey and Code Black contact card.
8	s47E(d) **- non-customer facing environment** + Read more ... In a non-customer facing environment, s 47E(d) **Staff response** s 47E(d) **ART response** s 47E(d)

	s 47E(d)

Responding to stalking and off-site harassment

Table 3: actions and processes that all staff and managers must take in response to an incident of stalking or off site harassment.

Item	Action
1	**Reporting stalking and off-site harassment** + Read more ... Any incidents of stalking, or harassment off-site (i.e. outside work) should be reported to police by a manager as soon as possible. Where there is uncertainty, seek advice from the Regional Security Advisers (RSA) by calling the Security Hotline. Not all stalking behaviour presents as menacing; some may come across as friendly e.g. an invitation for a drink. When a person feels they have been stalked, or harassed off-site, they should make their own detailed notes, including: s 47E(d) **Note:** the Security Branch **must** be notified of all incidents where a staff member has been stalked, or approached and harassed outside of work.
2	**Recording an incident of stalking, or off-site harassment** + Read more ... When a staff member is stalked or approached and harassed by a member of the public off-site or via any social media platform, because of their position with Services Australia, an incident must be recorded in the Customer Incident Management System (CIMS) or Customer Incident Recording Tool (CIRT). See Customer aggression – Reporting and recording incidents. Reporting the incident ensures the threat assessment conducted by the agency is based on complete and accurate information about the customer's behaviour. It also ensures the agency has evidence from the time of the incident should the matter be referred to police, or other legal action is commenced. Where a customer approaches a staff member on social media, the staff member must report this to their team leader or manager. This could include where a customer has recorded an interaction and posted it on social media. The social media policy for agency staff provides further information. If a customer's conduct has injured or impacted a staff member the incident should also be recorded in Our Safety. This ensures access to support for the staff member and an appropriate early intervention response. Work Health and Safety incidents can be found on the WHS incident reporting intranet page.
3	**Next steps for managers** + Read more ...

	Where an incident has occurred involving a staff member being stalked or approached and harassed by a member of the public, the manager should: s 47E(d)
4	**Protecting your own and other staff members' privacy** + Read more ... The privacy of staff members must be maintained at all times. Only the first name of a staff member should ever be provided to a customer, including when a customer asks for the full name. Any staff member who is concerned that a customer might obtain their full name, e.g. from a letter, should speak to their manager.

Responding to virtual threats to harm staff or damage agency property

Table 4: actions staff and site leaders take in response to phone threats to harm staff or property owned by Services Australia.

For threats to Employment Service Providers and other third parties, see Table 2 in Customer aggression – Escalating incidents.

When a threat is received through a telephone call, email, internet message, letter etc, use the following process.

Step	Action	Role
1	**Threat made by phone** + Read more ... When a threat to harm staff or damage agency property is made by phone: s 47E(d)	All staff
2	**Implement a malicious call trace (MCH)** + Read more ... A MCH can be activated in response to: • phone threats to harm staff or others (including any other organisation or person outside of the agency) • threats to property owned by Services Australia s 47E(d) Activate the process through s 47E(d) . s 47E(d)	All staff who use Services Australia Workspace

	s 47E(d) Go to Step 3.	
3	**Clarify the customer's statement and threat** + Read more ... s 47E(d)	All staff
4	**Notify team leader or manager** + Read more ... Immediately notify a team leader or manager of the threat s 47E(d) **Malicious call trace** - provide the team leader with the details collected. The team leader must immediately advise the Service Manager or Service Support Manager.	All staff
5	**Contact the customer** + Read more ... **Imminent threat with a known target** s 47E(d) **Imminent threat with an unknown target** s 47E(d) • If the customer cannot be contacted or refuses to withdraw the threat, go to Step 6 • If the customer withdraws the threat, go to Step 7 **Note:** access call recordings if appropriate to verify or clarify the threat. See Call and screen recording - information and access.	Site leader

6	**Call 000** + Read more ... Call the police immediately on 000 in the following circumstances: • contacting the customer is unsuccessful • the customer's identity is unknown • the customer refuses to withdraw the threat • it is decided a call trace is needed Tell the police the: • details of the threat • details of the person who made the threat • contact details for the manager at the threatened site The staff member who first received the threat should be available to give police additional details if required. Make sure the police reference number or details are recorded. Any additional information received from police should be given to the threatened site. Contact the threatened site to give them the details of the threat and tell them that police have been contacted. **Malicious call trace request and police follow-up** Ask the police to contact their State Communications Centre to have a request for trace faxed to Telstra's Trace Control Centre See Resources for the Services Australia Quick Reference Guide.	Site leader, Smart Centre Service Manager or Service Support Manager
7	**Contact Physical Security** + Read more ... A team leader or manager at the site who took the phone call should immediately contact Physical Security to discuss actions to be taken. In the unlikely event that Physical Security cannot be contacted, the site that received the threat should immediately contact the affected site and the police. See Resources for the Security Hub intranet page. Physical Security and the team leader or manager should consider: • the nature of the threat and location of the threat maker • if the customer is known to the site and their circumstances • previous incidents of customer aggression s 47E(d)	Site leader
8	**Record the incident** + Read more ... The staff member who received the threat and a site leader consult to record the incident on the customer's record. See Customer aggression - Reporting and recording incidents. If the incident results in a physical and/or psychological injury, it needs to be recorded in Our Safety. More information can be found on Reporting and Recording WHS incidents.	Staff member and site leader

Responding to written threats to harm staff or agency property

Table 5: process staff follow to respond to written threats to harm staff or damage property owned by the Service Australia.

Step	Action	Role

1	**Threat made in writing** + Read more ... Immediately notify a line manager when a threat to harm staff or damage agency property is made in writing.	All staff
2	**Contact the customer** + Read more ... A team leader or manager in the site the threat is made should immediately contact the customer to clarify the threat and seek a withdrawal. • If customer cannot be contacted or refuses to withdraw the threat, go to Step 3 • If the customer withdraws the threat, go to Step 5	Site leader
3	**Call 000 if contact unsuccessful** + Read more ... Immediately call the police on 000 if customer contact is not successful, the customer's identity is unknown, or the customer refuses to withdraw the threat. Contact the threatened site to provide details of the threat and advise police have been contacted.	Site leader
4	**Contact threatened site** + Read more ... A team leader or manager at the site where the threat was received should immediately contact the threatened site. The threatened site should immediately contact Physical Security to discuss actions to be taken. Consideration is given to: • the nature of the threat and location of the threat maker • if the customer is known to the site and their circumstances • previous incidents of customer aggression s 47E(d)	Site leader
5	**Record the incident** + Read more ... Staff member who received the threat and a site leader consult to record the incident on the customer's record. See Customer aggression - Reporting and recording incidents. Consider if a Managed Service Plan (MSP) is required, including consideration of the Notification Alert.	Staff member and site leader

Making a decision to lock the entrance to a site in response to a threat or incident

Table 6: reasons and considerations for managers and team leaders when making a decision to lock the entrance to a site in response to a threat or incident.

Step	Action
1	**Reasons for locking the entrance doors** + Read more ... Reasons for locking the entrance to a site include (but are not limited to): s 47E(d)

2	**Considerations before taking action to lock the entrance to a site** + Read more ... s 47E(d)

Responding to incidents related to infectious and/or communicable diseases

Table 7: actions staff take in response to incidents related to infectious and/or communicable diseases.

Stage	Incident response
Incident - Duress	**Duress - customer facing environment** + Read more ... Example behaviours: • Customer coughing towards staff • Customer spitting at the ground or towards staff • Threatening staff with an item that is or could transmit infectious/communicable diseases, for example a syringe • Intentional aggressive movements from a customer • Hostile or argumentative situation between customers • Customer refuses to leave the site after being asked • Customer aggression outside of office Staff response: s 47E(d) ART response: s 47E(d) Follow-up actions required: • Record an incident using relevant incident details. For example, Abuse - Actual - Verbal. See Table 1 > Step 4 and 5 on the General tab in Customer aggression - Reporting and recording incidents • For coughing and spitting incidents:

	◦ follow Workplace, Health and Safety directions. Refer to Infectious and communicable diseases ◦ record incidents of coughing towards staff using the behaviour type Assault No Weapon Actual ◦ record incidents of spitting not directed towards others using the behaviour type Health and Safety Actual Personal Health ◦ contact the Employment Law Team about the suitability of legal action and legal support. The Resources page has a link • Where police have been contacted, complete a Public Interest Release of Information form • An incident can also be recorded if the customer is unknown. See Table 2 > Step 3 on the General tab in Customer aggression Reporting and recording incidents • Consider implementing a Managed Service Plan • Record an Our Safety incident, if staff, contractors or customers are impacted (WHS Incident or Injury)
Incident - s47E(d)	s47E(d) **- customer facing environment** + Read more ... There is a direct physical threat that could result in injury. Example behaviours: • A person is spitting at staff, threatening to spit at staff, or infect others with a communicable disease • A person is in possession of, claims to be (or is suspected to be) in possession of a knife or weapon - not a firearm or flammable substance • A person is threatening to use an improvised weapon • Physical assault such as pushing, fighting, spitting and shoving, including between customers • Police use of force on site, including use of pepper spray, baton and other use of force Staff response s 47E(d) ART response s 47E(d) Follow-up actions required • Record an incident using relevant incident details. For example, Abuse - Actual - Verbal. See Customer aggression - Reporting and recording incidents • For actual or threats of spitting at staff or others: ◦ record the incident using behaviour type Assault-No weapon - Actual/Threat - Bodily fluids. Add additional behaviours as required ◦ follow Workplace, Health and Safety directions. Refer to Infectious and communicable diseases ◦ An incident can also be recorded if the customer is unknown. See Table 2 > Step 3 on the General tab in Customer aggression - Reporting and recording incidents • Consider implementing a Managed Service Plan

	• Record an Our Safety incident, if staff, contractors or customers are impacted (WHS Incident or Injury) • Consider contacting the Employment Law Team about the suitability of legal action and legal support. The Resources page has a link
Incident response - incidents in queues outside of the office/controlled entry	**Incidents outside - customer facing environment** + Read more ... A service centre may implement controlled entry to assist in managing physical distancing requirements and, as a result, queues may form outside the office. s 47E(d) Actions required: s 47E(d) An incident can also be recorded if the customer is unknown. See Table 2 > Step 3 on the General tab in Customer aggression - Reporting and recording incidents.
Person deliberately coughs or spits towards staff	**Person deliberately coughs or spits towards staff** + Read more ... An incident involving a person deliberately coughing or spitting towards a Services Australia worker (including a security guard) is considered to be an assault and may be prosecuted under relevant State, Territory or Commonwealth laws. Actions required: s 47E(d)
Filming, recording and photography	**Filming, recording and photography** + Read more ... Customers should be advised that Services Australia does not permit filming or recording of conversations within Service Centres. See Customer aggression - filming, recording and photography.

Satisfaction Research Program Security incident notification and escalation process

Table 8: actions staff take in response to incidents identified as part of the Satisfaction Research Program.

Step	Action
1	**What is a Security Incident?** + Read more ... A situation where a respondent's statement/s may indicate a risk to the safety of self or others, that is, threats of harm to staff, other people or the agency's property; or customers talking about suicide or self-harm. For example:

	s 47E(d)
2	**External Provider** + Read more ... Check whether the incident requires an emergency response. Call 000 in an emergency or life threatening situation, or when urgent police assistance is required, for example: • any situation where there is an imminent threat to the life or safety of a person (staff, customer or third party) • any incident which poses an immediate threat of danger to people or property, or • a bomb incident or threat **Note:** if an incident occurs outside business hours and you are unsure if it is emergency or not, contact the police. Provide the incident details to Satisfaction Research Program for follow up.
3	**Satisfaction Research Program/Strategic Customer Interactions Reporting** + Read more ... Send a referral email to the Customer Aggression Prevention Team (CAPT) with the following information included: • Incident channel/format (Computer Assisted Telephony Interview) • Date/time of incident • The Service Brand for which the provider was conducting the survey • Customer identifier (CRN/CSID/Medicare Number) • Verbatim comments/references. • A copy of the audio/transcript/metadata if available
4	**Customer Aggression Prevention Team (CAPT)** + Read more ... s 47E(d) • refer content to Social Work Services to request a review. Go to Step 5 **Customers talking about harming others or to damage property/buildings:** • refer content to the contact Physical Security Team to request a review and follow-up with the relevant zone Customer Aggression Network Operational Contact (CANOC). Go to Step 6
5	**Social Work Services** + Read more ... Undertake a professional assessment and determine the appropriate response for customers talking about self-harm. Record any aggression by the customer in the CIMS or CIRT. Where an incident has also been referred to the Physical Security Operations Team, Social Work Services will not attempt to contact the customer until Physical Security have provided advice. Where an ongoing need for support, or risk of aggression is prevalent, Social Work Services will refer to the relevant zone CANOC to consider implementation of a Managed Service Plan (MSP). Advise the CAPT of actions taken in response to the incident. Process for Social Work Services ends here.
6	**Physical Security Operations Team** + Read more ... Conduct a risk assessment of statements made by the customer and take response follow up action accordingly. Advise the CAPT and the applicable CANOC of actions taken. Document in CIMS/CIRT where aggression is prevalent.

	Process for Physical Security Operations Team ends here.
7	**Customer Aggression Network Operational Contact (CANOC)** + Read more ... Follow the established post incident process: • Record the incident (CIMS/CIRT) • Ensure Post Incident contact with the customer has occurred where appropriate and attempts to contact the customer are documented in CIMS/CIRT • Complete a business escalation if required • Consider and document reason of decision made to implement an MSP (CIMS/CIRT) • Consider triggering a Notification Alert Advise the CAPT of actions taken in response to the incident and outcome. Process for CANOC ends here.
8	**Record outcome** + Read more ... Advise Satisfaction Research Program of actions taken and the outcome of the incident.

References

Legislation

Links to the Federal Register of Legislation site go to an 'All versions' page. Select the 'Latest' version.

Privacy Act 1988

Public Order (Protection of Persons and Property) Act 1971 (POPPPA)

Work Health and Safety Act 2011

Resources

Emergency Response Procedures - Aggression (ERPA)

Emergency Response Procedures - Aggression (ERPAs) including s47E(d)

Workplace emergencies

Workplace emergency management

Workplace emergencies – Human-caused hazards or emergencies

Infectious/communicable diseases - intranet links

Infectious and communicable diseases

Infection control

Personal protective equipment (PPE)

Reporting and recording workplace health and safety (WHS) incidents

Phone bomb-threat checklist

Phone bomb-threat checklist (available on the Emergency Response Procedures – Aggression (ERPAs) including s47E(d) page)

Services Australia Workspace Quick Reference Guide

Services Australia Workspace > **Task Cards** > **Services Australia Workspace Quick Reference Guide**

Contact details

Customer Aggression Prevention Team (CAPT)

Services Australia Security Hotline

Security Hub

Customer aggression prevention networks and stakeholders

Research providers

Social workers referrals

Monitoring Operations

Public order (Protection of Persons and Property) Act 1971 links (POPPPA)

Ministerial delegations and authorisations (including Public Order (Protection of Persons and Property) Act 1971

Intranet links

Child Support Services, Delegations and Authorisations

Legal Issues - Customer Aggression

Customer Aggression Prevention Team (CAPT)

Satisfaction Research Programme

Security Branch

Services Australia Incident Management and Escalation Policy

Regional Security Advisers (RSA)

Training & Support

The agency's customer aggression training, the Managing Aggressive Behaviour Program (MAB Program) is mandatory for customer-contact staff and their direct supervisors.

Customer aggression prevention training further supports staff with 'Learning Bites' about preventing and managing customer aggression. 'The 4 WHYS to record' provides information to promote when and where staff record incidents of aggression and counterproductive behaviour. All customer aggression prevention Learning Bites and staff resources can be found by navigating to the relevant topic on the Customer Aggression Prevention Hub.

The Customer Aggression Training Summary outlines role required and recommended learning for; service delivery staff and their direct supervisors, staff who record, review and/or approve Managed Service Plans (MSPs).

CIMS role required learning is for all Centrelink service delivery staff and their direct supervisors. It is also role required for staff who record, review and/or approve Managed Service Plans (MSPs).

Australian Government
Services Australia

Customer aggression - Managed Service Plan (MSP) 104-07050000

Currently published version valid from 5/11/2025 12:43 AM

Background

s 22

This document outlines MSPs as a strategy to tailor customer services proactively or in response to incidents of customer aggression and counterproductive behaviour.

Managed Service Plans (MSP)

An MSP is an administrative action taken by Services Australia to tailor the way services are delivered to customers for:

- Centrelink
- Child Support
- Medicare

It can include:

- support options
- full or partial restriction of the customer's access to one or more service delivery channels

A service restriction is proportionate to the:

- severity of customer behaviour
- level of risk posed to staff safety

MSP decisions are approved by authorised decision-makers.

MSPs prioritise the safety of staff, balanced with the need to maintain access to payments and services provided by Services Australia.

Before proposing an MSP, follow all Emergency Response Procedures that apply to the aggressive or counterproductive incident. This makes sure that there is no immediate risk to the safety of staff, property and others.

For MSP process information, see:

- Managed Service Plan (MSP) - Proposing, recording and approving
- Managed Service Plan (MSP) - Implementing
- Managed Service Plan – s 47E(d) reviewing, non-compliance and one-off variation
- Managed Service Plan - Customer service delivered through a One Main Contact (OMC)

Types of MSPs

MSPs are put in place:

- after an incident of customer aggression, including when the behaviour is directed at another customer

- when the customer has shown counterproductive behaviour that could pose a risk to people's safety
- when a court order is in place that prevents the person attending our sites
- to help a customer who is experiencing vulnerability or barriers to accessing services without additional support

Reactive MSP

A reactive MSP with a restriction to service channels is used when there is ongoing risk to:

- people's safety
- agency property

This can include when a customer:

- has had multiple aggression incidents recorded in Customer Incident Management System (CIMS) or Customer Incident Recording Tool (CIRT) with a low severity rating
- threatens, physically harms or stalks staff
- has had one or more incidents recorded in CIMS or CIRT with a moderate or severe rating

Proactive MSP

A proactive MSP can be set up without a triggering incident of customer aggression. They can be used:

- when a customer experiencing vulnerability or barriers needs extra support to access Services Australia services. For more information, see Identifying customer vulnerability and risk issues
- to minimise any risk of customer aggression or counterproductive behaviour, such as when circumstances pose a risk (adverse decision, anniversary of a negative life event)
- if the agency gets information from a specialist officer (for example, Job Capacity Assessor/service officer in Face to Face Incarcerated Customer Servicing team) that indicates a potential risk of violence
- when a third party informs the agency that there is a risk of aggression. A third party can include a mental health unit, corrective services, a shared premises partner, or Employment Services Provider

A proactive MSP can include service channel restrictions if the available information shows that staff safety may be at risk. Each case must be considered on a case-by-case basis.

Discussions about MSPs and servicing strategies with a customer should be supportive and positive. Customer input and engagement is more likely to lead to an effective MSP, and the customer's insight into their individual circumstances will help the agency make a more transparent and respectful decision.

The length of the plan will depend on how much time is needed to make sure the service strategies are effective. See MSP timeframes.

Note: an MSP may extend beyond 12 months to align with court order timeframes, or a period of a week beyond an incarceration release date to provide support and manage ongoing customer interactions.

Administrative strategies

Administrative strategies let the agency tailor an MSP to help with managing a customer. This can include restricting a person's access to one or more service delivery channels. This option is open to the agency regardless of whether the person is a customer.

A One Main Contact (OMC) or Personalised Services Service Officer (PSSO) is assigned to support internal and external servicing strategies. These include:

- managing enquiries from the customer and resolving issues in a timely and procedurally accurate manner
- making sure that all decisions and options are clearly explained to the customer
- working closely with delegates, specialist staff and external agencies to offer a holistic service experience and achieve quality outcomes for the customer
- working with customers until they are ready to be transitioned back to contacting the agency through usual methods and self-managed services

See Managed Service Plan (MSP) - Proposing, recording and approving.

MSP timeframes

The length of an MSP will be based on:

- the severity of the incident and level of risk posed to staff safety
- the time needed to make sure the service strategies are effective

Provisional MSP: 1-10 business days (Centrelink only)

A Provisional MSP is an immediate risk management strategy to keep staff, others and property safe, following an incident of customer aggression or counterproductive behaviour:

Provisional MSP timeframes are:

- 1 5 days for low severity and low future risk of aggression incidents
- 6 10 days for serious, moderate or multiple incidents of aggression. This is to give the agency enough time to make a decision about a longer term MSP

The timeframe allows for:

- a period for the customer to de escalate
- time to make sure that staff, customers, and others are safe
- time to contact the customer to resolve any outstanding business or triggers for aggression, discuss behavioural expectations and assess the risk of further aggression. (See Customer aggression Post incident contact)
- when there is a future risk, time to convene a Local Assessment Panel (LAP) to assess if a longer term MSP is required, including service restrictions and service support strategies

A provisional MSP will always include a restriction to one or more service channels.

See Resources for Customer Aggression Network Operational Contacts (CANOC) and LAP structures.

Note: when a provisional MSP runs over public holidays CIMS will not take them into account. This may limit the number of working days to assess and implement a long term MSP.

Long term MSP: 11 business days to 12 months

- Reactive MSPs should be in proportion to the severity of customer behaviour and level of risk posed to staff safety
- Proactive MSPs should take into consideration how much time may be needed to be sure that the service strategies are taking effect. These strategies are explained in detail in Proposing and recording a MSP

The Customer Aggression Prevention Team (CAPT) can provide advice and support for developing MSP timeframes. Resources has a link to the Customer Aggression Prevention page for CAPT's contact details.

Greater than 12 months (court orders and incarcerated customers)

When any court-issued order is in place, the MSP timeframe must align with the period of the court order.

For incarcerated customers, the MSP may be implemented for a period of a week beyond an incarcerated release date. This is to provide support and manage ongoing customer interactions.

Safety alert

A safety alert is a feature of the MSP warning message. It alerts staff to MSP customers who have a history of customer aggression incidents with a behaviour type recorded in the Customer Incident Management System (CIMS) of:

- actual or attempted assault, or
- actual stalking

Where there **is verified information** indicating a potentially high risk of assault occurring to agency staff, s 47E(d) [redacted]

An active safety alert supports staff decision making for customer management and service centre response.

Notification Alert (Centrelink Only)

The Notification Alert feature of the MSP is designed to enhance safety by enabling the storage and sharing of images between service centres of customers who have committed or threatened serious aggression.

When active, the Notification Alert appears in the Front of House application (FoH App) within Virtual Waitrooms (VWR) of selected service centres. This alert can be issued with or without a CCTV image of the customer, providing staff with crucial information. The Notification Alert displays customer details, including their name and CRN, and the option to view an image of the customer, (if one has been linked). A notification email includes a link to view the customer's MSP within the Customer Incident Management System (CIMS), along with any servicing arrangement details.

Local Assessment Panels (LAPs) and Zone Assessment Panels (ZAPs)

Local Assessment Panel (LAP)

Before the end of the provisional MSP, a LAP must meet to work out if a long term MSP is needed. The panel should decide on the length of the MSP and propose any channel restrictions and service strategies.

The Service Centre Manager (SCM) or another leadership member convenes a LAP. The SCM can liaise with Zone CANOC if support is required.

Zone Assessment Panel (ZAP) - Centrelink

A ZAP must meet at least monthly. The trigger for a panel is determined by the Zone. Examples of a trigger include:

- within 24 48 hours of a serious incident
- in line with review dates of MSPs
- when the need for a new MSP is identified

The ZAP's chair is a Customer Aggression Network (CAN) representative or another leadership member, such as a Region Manager. The CANOC must record the panel's decisions.

See Resources for LAP and ZAP structures.

When to refer for an MSP

An MSP must be put in place when a customer poses an ongoing risk to staff safety. An ongoing risk to staff safety includes when:

- a customer has had multiple incidents of customer aggression
- a customer has used violence
- a customer has harmed or threatened to physically harm staff or others
- a customer has stalked a staff member or otherwise made them feel unsafe off-site
- the severity of an incident is moderate or serious
- the agency receives information from a specialist officer indicating a potential risk of violence, such as a Job Capacity Assessor or service officer in Face to Face Incarcerated Servicing team.
- information from a third party indicates a risk of aggression that needs to be managed. Third parties can include a partner agency or job provider
- CAPT identifies a customer as high risk through proactive data analysis

Customers with identified vulnerabilities or barriers may have an MSP to give them extra support to access agency services. Proactive MSPs can include internal and external referrals, and a holistic focus on supporting the customer to address their barriers and vulnerabilities.

How to refer for an MSP

For information about proposing MSPs for different business areas, see Managed Service Plan (MSP) – Proposing, recording and approving.

Shared premises with partner agencies

Services Australia collaborates with partner agencies to decide on how to serve customers accessing shared premises. All staff located in shared premises must deliver services in line with MSP arrangements.

After an incident of aggression in a shared premises, Services Australia and partner agencies have agreed to:

- share information
- undertake risk management according to their respective policies and procedures

This may include limiting a customer's contact options, either independently or through a joint MSP. A Local Assessment Panel (LAP) is the agreed forum to share information and assess risks.

Restricting face-to-face service at a premises requires the leaseholder's agreement.

Customers cannot access partner agencies' services if they have either or both of:

- a Services Australia service channel restriction that prevents them from entering a shared premises
- a service channel restriction with a partner agency

Protection orders (including family violence orders) between staff and customers

A protection order is a legal order with rules about how a person (the respondent or defendant) is allowed to act towards somebody else (the protected person). This is to keep the protected person safe from physical, verbal and emotional abuse.

An order can come from a court, or in some cases from police.

A protection order about family and domestic violence is recognised throughout Australia. It can be enforced in any state or territory.

Protection orders have different names in each state and territory.

- **Australian Capital Territory:** Domestic Violence Orders, Personal Protection Orders
- **New South Wales:** Apprehended Domestic Violence Orders, Apprehended Personal Violence Orders
- **Northern Territory:** Domestic Violence Orders, Personal Violence Orders
- **Queensland:** Domestic Violence Orders, Peace and Good Behaviour Orders
- **South Australia:** Intervention Orders
- **Tasmania:** Family Violence Orders, Restraint Orders
- **Victoria:** Family Violence Intervention Orders, Personal Safety Intervention Orders
- **Western Australia:** Family Violence Restraining Orders, Misconduct Restraining Orders

A staff member may tell the agency that they hold a protection order in their private personal capacity (as the protected person) against a customer.

Under the Work Health and Safety Act 2011, the agency must:

- ensure the safety of workers
- ensure that the safety of others (including customers) is not put at risk as a result of the agency carrying out its business, so far as is reasonably practicable.

How to fulfil these obligations will depend on the circumstances of each case.

When a staff member discloses that they hold a protection order, the relevant business areas should conduct a risk assessment to understand more about the situation and existing mitigation strategies. The business area should do this in consultation with the staff member and Security Branch.

After assessing the situation, and if the staff member agrees, the agency may implement an MSP with alternative servicing arrangements for the customer.

For more information see Managed Service Plan (MSP) – Proposing, recording and approving – Process, Table 1, step 14.

MSP SMS (Centrelink customers only)

To reduce the risk to staff safety, customers must be notified of the MSP decisions as soon as possible.

Whenever possible, customers should get an SMS before they get more detailed information in an MSP letter. See Centrelink letter online and Electronic Messaging.

Because the information provided in an SMS is limited, the messages are intended to complement and not replace an MSP letter.

Only approved decision makers can send an SMS, and only in the following circumstances:

- when the customer cannot be contacted by phone
- the phone discussion with the customer was unproductive
- the phone contact was successful and the approved decision-maker decides the customer may benefit from confirmation of MSP details by SMS
- if waiting until the next day to call the customer may result in a more productive discussion and the customer would benefit from a preliminary message
- customer may benefit from having a One Main Contact or Personalised Services officer's numbers saved on their mobile phone

s 47E(d)

s 47E(d) See Customers talking about suicide or self-harm.

If there is family and domestic violence involving an immediate threat to safety, staff must follow their local response guidelines. s 47E(d)

s 47E(d) See Family and domestic violence.

MSP letters

To reduce risk and maintain staff safety, customers should find out about any servicing restriction as soon as possible.

Customers should get letters:

s 47E(d)

When Personalised Services manages an MSP as part of the direct referral process, they will issue the relevant MSP letter.

For information about MSP letter delivery methods, see Managed Service Plan (MSP) Implementing.

Where services are to be delivered through an OMC/PSSO, a Services Australia contact card must be issued to an MSP customer. This ensures they know who their OMC/PSSO is and how to contact them.

See Resources for a link to the Ordering business cards, employee contact cards page.

MSP letters can be translated. For more information, see Translation of documents.

Approving MSPs

Reactive or proactive MSPs must be approved by an approved decision maker.

Proactive MSPs that **do not** include service channel restrictions must be discussed at the Local Assessment Panel (LAP). When the relevant Zone CANOC is not implementing the MSP, they must be advised before implementation.

Staff with the CIMS Manager role can propose and implement longer term MSPs involving service strategies and referrals, but not service channel restrictions. They can also propose and implement provisional MSPs (1 to 10 business days).

See Managed Service Plan (MSP) - Proposing, recording and approving.

Warning message displays on customer record after a CIMS MSP is active

The **warning** message will appear in:

- Customer First
- Process Direct
- Front of House Application

The warning message will display when **there is an active Services Australia MSP in place and** the customer's record is first accessed.

Where there is also an active Department of Employment and Workplace Relations (DEWR) MSP in place, the warning message **gives** staff access to the content.

If no active Services Australia MSP exists and DEWR has an active MSP in place, the warning will not display to staff.

Where an active Services Australia MSP is in place the warning will appear via:

- Customer First
- Process Direct
- Front of House Application
- the work item received from Workload Manager (WLM)

s 47E(d)

The message shows any:

- safety alerts
- service channel restrictions

- contact officer details, and
- the end date of the MSP

MSP warning banners in Q-Flow

Q Flow displays a warning banner for:

- an active safety alert
- any possible active Services Australia or DEWR MSPs. Applicable MSPs, including any service channel restrictions, can then be accessed and viewed via Process Direct

Sensitive Information alert (Medicare public customers only)

CIMS MSPs are referenced in a **Sensitive Information Indicator** in the Consumer Directory Maintenance System (CDMS) at the Personal level.

When staff access a customer's record in CDMS and a Sensitive Information alert displays, they must check the Sensitive Information Indicators on the s47E(d) .

Customers with an MSP have one of the following Sensitive Information Indicator types:

- Full service restrictions
- Partial service restrictions

The indicator shows any service channel restrictions and One Main Contact arrangements for the customer.

See Sensitive Information Indicators in the CDMS for more details.

CIMS Security Roles

The MSP warning message will display to all staff, regardless of their CIMS Security role.

See Accessing and using the Customer Incident Management System (CIMS) for how to request access to CIMS. This has information about the functions that can be performed when staff hold each CIMS Security role.

Collaborative service strategies across service centres and Smart Centres

Service centres and Smart Centres work together to develop the most appropriate service strategy to:

- manage customer interactions and behaviour
- mitigate the risk of future aggression incidents

If an incident of customer aggression or counterproductive behaviour happens over the phone, Smart Centre team leaders and managers should contact the relevant Zone CANOC to discuss the best approach to deliver services to customers.

Note: if an incident involves a threat, emergency procedures must be followed. See Customer aggression - Response.

Applying an MSP with restrictions across service delivery brands

Before setting up an MSP with restrictions, the approved decision maker should consider if the restriction should apply across al service brands.

See Personalised Services and Managed Service Plan (MSP) - Proposing, recording and approving.

Services Australia Agents and Access Points

s 47E(d)

. Services Australia will support the host organisation by providing alternate methods for the customer to access services. See the National Agent and Access Point SharePoint page on Customer Aggression.

Employment Services Provider MSPs

Employment Services Providers can set up their own MSPs for job seekers. When a provider puts an MSP in place, the Department of Employment and Workplace Relations (DEWR) will transfer details about it into CIMS.

Provider MSP details sent by DEWR are:

- MSP ID
- MSP status
- MSP start and end dates
- One Main Contact (OMC) User ID
- Backup User ID
- Type of MSP
- Related Incident ID
- Servicing strategies
- Restriction details:
    - Service Channel of restriction/s
    - Level of restriction/s
    - Restriction notes

The provider's MSP details are in CIMS. To search for Incident and Managed Service Plan records, see Accessing and using the Customer Incident Management System (CIMS), Process page > Table 3.

Provider MSPs do not affect the way a customer can deal with Services Australia. They may be useful when:

- talking with a customer about dealing with their provider
- identifying potential risk to the safety of Services Australia staff.

Non-compliance with service restrictions

If a customer contacts the agency through a restricted service channel, they have not complied with their MSP. Serving these customers can encourage them to keep breaching their service restrictions.

When a customer breaches their MSP, the first priority is to remove them from the premises as quickly as possible. If a customer's behaviour escalates or is aggressive, follow the site Emergency Response Procedures Aggression (ERPAs).

A review of the current MSP may also be required. Depending on the severity of the non compliance and whether the customer's circumstances have changed, give consideration to convening a LAP.

See:

- Managed Service Plan (MSP) - Reviewing
- Managed Service Plan (MSP) - Customer not complying

One-off variation in exceptional circumstances

s 47E(d)

See Managed Service Plan (MSP) - One-off variation.

Requesting support

When staff are developing MSP proposals, they can ask for policy advice from the CANOC, CAPT, or other specialists. This includes extended MSP timeframes up to 12 months. See Resources for CAPT contact details.

The Resources page contains links to:

- staff roles and responsibilities in relation the Customer Incident Management System (CIMS)
- the Services Australia website
- intranet pages about managing incidents of customer aggression and counterproductive behaviour
- CANOC and CAPT contact details
- LAP and ZAP structures

Contents

Managed Service Plan (MSP) Implementing

Managed Service Plan (MSP) One off variation

Managed Service Plan (MSP) Proposing, recording and approving

Managed Service Plan (MSP) Reviewing

Related links

Customer aggression Prevention and management

Accessing and using the Customer Incident Management System (CIMS)

Customer aggression Response

Customer aggression Staff support

Identifying customer vulnerability and risk issues

Centrelink letters online and Electronic Messaging

Sensitive Information Indicators in the CDMS

Notification Alert

References

Legislation

Links to the Federal Register of Legislation site go to a 'Series' page. Select the ‘Latest’ version.

Child Support (Registration and Collection) Act 1988

Human Services (Medicare) Act 1973

Public Governance, Performance and Accountability Act 2013

Public Order (Protection of Persons and Property) Act 1971 (POPPPA)

Social Security (Administration) Act 1999

Work Health and Safety Act 2011

Resources

Roles and Responsibilities

The Customer Incident Management System page includes the staff roles and responsibilities in relation the Customer Incident Management System (CIMS).

Local Assessment Panels (LAPs) and Zone Assessment Panels (ZAPs) Structures

The following explains the purpose and structure of LAPs and ZAPs.

Local Assessment Panels (LAPs)

Table 1

Category title	Description
Purpose of LAPs	- Assess ongoing staff safety risk immediately following incidents of aggression - Ensure appropriate post incident action has occurred - Monitor Managed Service Plans (MSPs) for site customers - Monitor progress of MSPs for site customers (e.g. servicing strategies, - breaches) - Refer cases to Zone Panel as necessary - Manage site based One Main Contacts (OMCs) - Determine if a Notification Alert should be extended or ceased
LAP Membership composition	- Service Centre Manager (SCM) or another leadership member chairs the LAP - Site leadership (as available) - Social Worker - Specialists as relevant (e.g. Indigenous Services Officer, Multicultural Services - Officer, Community Engagement Officer) - Zone Customer Aggression Operational Contact (CANOC) member if - needed - OMC/Personalised Services Service Officer (PSSO) (at minimum seek input)
LAP Frequency	- LAPs are convened ad-hoc as needed or at a minimum monthly. This ensures that the progress of current MSPs are monitored against servicing strategies and MSP compliance - LAPs should be convened within 48 hours of an incident. This ensures that any reporting requirements are met, e.g. WHS incidents, recording in CIMS. As well as to assess any active Notification Alerts (including the duration), and propose whether any further service channel restrictions and servicing strategies are required - LAP may convene following a breach of restriction
LAP Preparation and meeting	- Information to be collated and distributed to LAP members beforehand as needed e.g. pattern of previous behaviour, MSP history, relevant background - LAP meetings can take place via teleconference and/or face to face - Chair should ensure that minutes are taken and any action items d stributed to panel members via email - CANOC and Region Manager should be notified of the panel outcomes - Any decisions need to be recorded in either the incident record or MSP (e.g. where no further MSP will result, record how risk has been assessed and addressed in an incident note) - Consideration of a template to be used to be copied into the MSP notes - The need for future meetings are decided when customer's circumstances change, when there is a breach of restriction or when there is disagreement between panel members
LAP Accountability and visibility	- SCM or another leadership member to ensure LAP meeting action items are followed up - SCM can liaise with CANOC if support is required to finalise LAP meeting action items

Zone Assessment Panels (ZAPs)

Table 2

Category title	Description
Purpose of ZAPs	- Assess risk and ongoing customer management options - Make recommendations on MSPs - Review MSPs
ZAP Membership composition	- Customer Aggression Network (CAN) representative or another leadership member (e.g. Region Manager) chairs the ZAP - CANOC to perform secretariat functions - Social Worker

	• Specialists as relevant, (e.g. Forensic Psych, Indigenous Services Officer, Multicultural Services Officer, Community Engagement Officer) • OMC/PSSO • CAPT account manager for Service Zone as needed for complex cases • SCM of impacted site where appropriate
ZAP Frequency	• ZAPs should be convened at a minimum monthly • Trigger for panel can be determined by the Service Zone (e.g. within 24-48 hours of a serious incident; in line with review dates of MSPs, when the need for a new MSP is identified
ZAP Preparation and meeting	• CANOC/Operational Management teams to prepare agenda • Agenda should consist of the details of MSPs due for review and any new cases • Meetings will generally be by teleconference • CANOC to take minutes and ensure decisions are documented thoroughly to inform subsequent documentation within MSP • CANOC will distribute minutes to panel members and communicate any action items. CANOC will coordinate follow-up on action items within the set timeframes, including coordinating any necessary coding of MSPs or other actions on customer records
ZAP Accountability and visibility	• Panel chair should ensure the Service Zone National Manager has visibility of panel outcomes • Panel chair should ensure relevant Service Zone Region Managers have visibility of panel outcomes

Intranet links

Agent and Access Points

Customer Aggression Prevention

Customer Incident Management System

Customer Incident Recording Tool

Emergency plans and customer aggression emergency response procedures

Health and Safety

Legal Services Division

Ministerial delegations and authorisations

Ordering business cards, employee contact cards, name badges and desk plates

Services Australia Incident Management and Escalation Policy

Shared premises safety - WHS considerations

Security for Service Centre Managers

Smart Centre Escalations (POT referral)

Employee assistance program

Services Australia website

Our service commitments

Your responsibilities

Payment and Service Finder

Contact details

Customer Aggression Prevention Team (CAPT)

Customer Aggression Network Operational Contact (CANOC) role

Training & Support

Add the course number to the s 47E(d field in the s 47E(d) in ESSentials:

- s 47E(d) CIMS: Introduction to MSPs

Australian Government

Services Australia

Managed Service Plan (MSP) - Proposing, recording and approving 104-07050010

Currently published version valid from 18/11/2025 8:31 PM

Background

s 22

s 47FE(d)

This document contains the process staff use to propose, record and approve a Managed Service Plan (MSP). MSPs with service channel restrictions are considered Services Australia wide.

If someone is a customer of more than one service brand, and they pose a risk to more than one service brand, they must have a One Main Contact (OMC) or Personalised Services Service Officer (PSSO) assigned.

Who can propose, approve, and activate an MSP

Staff with the CIMS Manager and Delegate roles can:

- propose an MSP with restrictions or a Personalised Services referral
- initiate and activate an MSP which contains only servicing strategies

Provisional MSPs - Staff with the CIMS Manager or Delegate access role can create a provisional MSP. It will become active once the MSP is saved and submitted. Provisional MSPs are implemented by the Face to Face Service Delivery Support Team (F2F SDST).

Long-term MSPs - Staff with the CIMS Delegate access role can activate a long-term MSP by approving proposed service channel restrictions. Long term MSPs are recorded and activated by Face to Face SDST.

Personalised Services staff with the CIMS Manager role can initiate and activate an MSP by approving a proposed Personalised Services referral.

Also see Customer Aggression – Managed Service Plan (MSP), letter and SMS decision makers.

Proposing an MSP

See Customer aggression - Managed Service Plan (MSP) for detailed information.

How an MSP is implemented

An MSP can be implemented after an incident of customer aggression or counterproductive behaviour, including when the behaviour:

- is directed at another customer
- has been identified as a future risk of aggression

It could also be implemented to help a customer who has:

- self-identified vulnerabilities or barriers

- contacted through Escalated or External Complaints, Media Branch, National Restricted Access Team (NRAT), Senior Executives, Smart Centres, Social Work Services or Intelligence and Investigations, or identified as high risk through proactive data analysis

MSP timeframes

A Provisional MSP is implemented as an immediate response to an incident of customer aggression or counterproductive behaviour:

- 1 5 business days for low severity and low future risk from incidents of aggression
- 6 10 days for serious, moderate or multiple incidents of aggression

Note: when implementing a Provisional MSP for a period including public holidays, incident systems will not identify and take into account public holidays. This may limit the number of working days to assess and implement a long term MSP.

A long-term MSP is implemented as a strategy to provide support and manage ongoing customer interactions:

- 11 business days to 12 months
- Greater than 12 months to align with court order timeframes, or a period of a week beyond an incarcerated release date to provide support and manage ongoing customer interactions

Approvals

MSPs must be approved by an approved decision maker. Approvals vary depending on the type and length of the MSP.

Medicare Public and Centrelink Face to face

Local Assessment Panel (LAP)

s 47E(d) should convene a LAP within 48 hours of an incident or where a customer experiencing vulnerability or risk issues is identified and may benefit from proactive management.

The purpose of the panel is to assess any ongoing risk to staff or others, and to make sure the risks posed by the customer are mitigated. The panel should make recommendations about the duration of the required MSP and consider and propose channel restrictions and servicing strategies. The s 47E(d) can liaise with Zone Customer Aggression Operational Contact (CANOC) if support is required.

Zone Assessment Panel (ZAP)

A Customer Aggression Network (CAN) representative or another leadership member, e.g. Region Manager should convene a ZAP at a minimum monthly. The Service Zone determines the event that triggers the panel. For example, within 24 - 48 hours of a serious incident, in line with review dates of MSPs, or when the need for a new MSP is identified.

The purpose of the panel is to assess risk and ongoing customer management options, make recommendations on MSPs and to review MSPs.

For more information about Local and Zone Assessment Panels, see Customer aggression – Managed Service Plan (MSP).

For a list of CAN members, see the Resources page for a link to the Customer aggression prevention - networks and stakeholders page.

Centrelink Smart Centres

Smart Centre Team Leaders and Managers should contact the Customer Response Team to propose an MSP. The Customer Response Team will make MSP recommendations to the relevant Zone CANOC. Refer to the Smart Centre Escalations SharePoint page including a link to the MSP referral form. See Resources page under Intranet links.

Child Support

Personalised Services offers intensive case management to help Child Support customers with the most complex needs or escalating behaviour. It provides a single point of contact for the customer while their issues are being resolved. See Customer referral guidelines for Child Support staff.

Medicare Public Customers, Telephony

s 47E(d) should discuss MSP referrals with the Health Services Delivery Division (HSDD) CANOC. HSDD CANOC will assess the incident and refer to the Zone CANOC if:

- there is a risk to face to face services
- there are previous incidents of aggression in the face to face environment in the last 12 months

- is already being managed by the zone

The HSDD CANOC will set up MSPs for telephony only customers.

Medicare Public Customers, Service Centre

The s 47E(d) should discuss any MSP referrals with the Zone CANOC.

The HSDD CANOC must be notified of any MSP implemented for a Medicare customer.

Medicare Provider Customers

Team Leaders and Managers should discuss MSP referrals with the HSDD CANOC.

See Resources for CANOC details.

Smart Centre Social Work Services

Smart Centre Social Workers should contact the Customer POT to recommend an MSP. The Smart Centre Customer Portfolio Operations team will submit requests for an MSP to the relevant Zone CANOC. Refer to the Smart Centre Escalations SharePoint page including a link to the MSP.

Appeals Branch

If an Appeals Branch staff member identifies that an MSP is needed for a customer, either after recording an aggression incident or identifying complex needs, vulnerabilities, or a risk to staff safety. Appeals Branch staff should contact the relevant Zone CANOC to discuss the recommendation. See the Resources page for contact details.

Assessment Services

Assessors play an important role in identifying vulnerabilities, barriers and/or the risk of aggressive behaviour.

To keep other agency staff safe, Assessors can recommend that an MSP be implemented after experiencing an incident or after using the Risk Assessment Tool.

Assessors may discuss a proposed MSP with the Service Centre Manager and if appropriate, contact the Zone's Customer Aggression Network Operational Contact (CANOC).

Resources has a link to the Handout Risk Assessment Tool and Zone CANOC contact details.

Shared premises

Services Australia shares a number of service centres with other Commonwealth agencies, not for profit organisations and State Government entities. Restricting face to face servicing to a premises requires agreement of the premises holder. Where a mutual customer is involved in an incident, a representative of the partner agency must be included in the Local or Zone panel discussion. This may result in Services Australia and the partner agency implementing a joint MSP.

Service Delivery Partners MSP referrals

If a Service Delivery Partner determines that an MSP is needed after recording an incident of customer aggression, a Team Leader or Manager of that site should email the Smart Centre Customer Portfolio Operations team, who will liaise with the relevant Zone CANOC.

If a business area needs to contact a Service Delivery Partner about a customer or to discuss an MSP they should email Capability Improvement team. Resources has a link to contact details.

See also Managed Service Plan (MSP) - Implementing.

Recording an MSP

MSPs are recorded differently in the Centrelink, Child Support and Health Service Delivery Division systems depending on the service brand the customer is accessing.

Staff with the CIMS Manager role record the MSP proposal after a LAP or ZAP has convened to make sure all relevant information has been considered and specialist advice has been sought where appropriate.

See Process for instructions on how to record an MSP.

Service Channel Restrictions

Services Australia can restrict one or more service channels fully or partially, providing various ways of limiting a person's contact with the agency and to assist with managing the impact of customer aggression and counterproductive behaviours.

Service channel restrictions:

- must be appropriate to individual circumstances of a customer. For example, the customer must have access to the channel and have previously used this to complete their business
- must be proportionate to the person's conduct   for example:
  - serious and/or repeat incidents of aggression should result in a face to face service channel restriction;
  - repeat phone incidents should result in a partial phone restriction; and
  - repeat and serious phone incidents should be considered for full phone restrictions
- must be based on a risk assessment   the likelihood and consequences of another similar or more serious incident of aggression s 47E(d)

s 47E(d)

- should be considered within the broader framework of the Preventing and managing Customer Aggression Policy, and
- may be used in conjunction with other strategies or as a stand alone strategy where necessary   for example as part of a Provisional MSP

The agency has the right, as the occupier of Commonwealth premises, to withdraw its consent for any person to come on to Commonwealth premises. References has more information.

Note: a service channel restriction does not prohibit the agency from contacting the customer where necessary and safe to do so. Contact with the customer must be coordinated with the One Main Contact (OMC) or Personalised Services Service Officer (PSSO) where one has been assigned.

For processing staff completing electronically assigned work, it is necessary to contact the OMC or PSSO before completing the work item.

Resources has a table demonstrating the types and levels of service channel restriction.

Customers may be restricted to contacting the agency:

- at prescribed time periods
- on certain days of the week
- number of contacts
- in writing only
- on specific contact numbers, including via call customisation
- through an email redirection

s 47E(d)

-
- . See Urgent payments due to exceptional and unforeseen or extraordinary circumstances

Referrals to Personalised Services

The national Personalised Services team objectives include:

- providing a dedicated point of contact (OMC) between the customer and Services Australia
- managing the customer by phone and online servicing to reduce the impact of aggressive behaviour on customers and staff in service centres/smart centres
- managing persistent complainants to restrict any negative impacts on the business
- improving customer and business outcomes by:
  - a collaborative approach to complex case management, and
  - external referrals
- supporting customers through crisis
- enabling the customer to resolve their issues and meet responsibilities through self-managed services
- correcting errors and address systemic service issues
- providing the customer and stakeholder with appropriate strategies to support customers experiencing vulnerability and risk issues

Referrals to Personalised Services can be made as part of an MSP following an incident of customer aggression or counterproductive behaviour or as a proactive service strategy to assist staff experiencing complex or vulnerable issues.

For Centrelink customers and Medicare Public face to face customers, referrals to Personalised Services can be made through Customer Incident Management System (CIMS).

Proposals for customer management by Personalised Services can be made as part of an MSP in response to the following circumstances:

- Following an incident of customer aggression or counterproductive behaviour including where the behaviour is directed at another customer or the customer has displayed counterproductive behaviour which could pose a risk to staff safety
- Where a customer has:
    - identified vulnerabilities or barriers, or
    - been directly referred by Health Services Delivery Division, Escalated or External Complaints, Media Branch, National Restricted Access Team (NRAT), Senior Executives, Smart Centres, Social Work Services or Intelligence and Investigations, or where the customer is identified as a future risk of aggression through proactive data analysis.

Proposals and referrals for proactive Personalised Services management are limited to customers with **no**:

- current restrictions on accessing agency services
- incidents of aggression in the last 12 months within the face to face environment
- current case management by the Service Zone
- identified risk to face to face staff

Making the referral

Child Support customers See Customer referral guidelines for Child Support staff Referrals to the Personalised Services Team table.

Centrelink customers and Medicare face to face customers Referrals to Personalised Services can be made as part of an MSP following an incident of customer aggression or counterproductive behaviour or to assist a customer experiencing vulnerability or risk issues.

Centrelink Smart Centre Team Leaders and Managers should contact the Customer POT to refer a customer to Personalised Services. Refer to the Smart Centre Escalations SharePoint page including a link to the MSP referral form.

Health Service Delivery Division customers - if the customer is a:

- public customer telephony only - MSPs implemented by HSDD CANOC will be managed by Personalised Services based on the proactive proposals and referrals criteria outlined above
- public customer - referrals to Personalised Services can be made as part of a reactive MSP following an incident of customer aggression or counterproductive behaviour or as a proactive servicing strategy (as part of a proactive MSP)
- provider customers (Medical Doctor, Aged Care) contact HSDD CANOC

Direct referrals from Escalated or External Complaints, Media Branch, National Restricted Access Team (NRAT), Senior Executives, Smart Centres, Social Work Services or Intelligence and Investigations, HSDD CANOC, or where the customer is identified as high risk through proactive data analysis. See Personalised Services referral guidelines.

See also:

- Personalised Services
- Referring customers to and handling enquiries and correspondence for Personalised Services

Other internal referrals can be made to specialists and program areas such as Social Worker, Community Engagement Officer or Appeals.

For Child Support customers, referrals to Personalised Services can be made through Cuba. See Customer Referral Guidelines (CRG) - Child Support > Personalised Services Referrals.

For Health Services Delivery Division customers, referrals can be made via local Service Zone Customer Aggression Network (CANOC).

Service strategies, including internal and external referrals

As part of the Local, Zone or HSDD Assessment Panels, panel members or other staff within the agency can recommend a variety of other strategies to assist customers. These strategies allow for further tailoring of MSPs to assist ongoing customer management and include both internal and external referrals, as well as some payment options to mitigate the impacts of customer vulnerabilities, for example weekly payments.

Consultations which occur prior to the MSP proposal assist in providing visibility of the risk assessment process used to inform MSP recommendations.

Internal referrals can be made to specialists and program areas such as:

- Social Work Services
- Indigenous Services
- Appeals
- Family and domestic violence

External referrals can include (but are not limited to):

- Legal Aid
- Counselling Services
- Housing assistance

Resources page has links to useful information including the Payment and Service Finder tool.

Employment Services Provider MSPs

Employment Services Providers can implement their own MSPs for their customers. Where a Provider implements an MSP, details of the MSP will be transferred to CIMS from the Department of Employment and Workplace Relations (DEWR).

Provider MSP details sent by DESE are:

- MSP ID
- MSP status
- MSP start and end dates
- One Main Contact (OMC) User ID
- Backup User ID
- Type of MSP
- Related Incident ID
- Servicing strategies
- Restriction details
    - service channel of restriction/s
    - level of restriction/s
    - restriction notes

Details of the Provider MSP can be located via CIMS. Provider MSPs do not impact the way a customer can deal with Services Australia but may be useful when providing advice to customers on dealing with their provider and identifying potential risk to the safety of Services Australia staff.

Approving MSPs

Approved decision makers vary depending on the type and timeframe of the MSP.

Approved decision makers can contact the Customer Aggression Prevention Team (CAPT) for support and advice. See Resources for a link to the CAPT intranet page.

Notification Alert

A Notification Alert can only be triggered for a customer who has an active Managed Service Plan (MSP).

A Notification Alert should be considered when a customer has had a recent incident recorded in the Customer Incident Management System (CIMS) that has the potential to significantly impact the agency's business or operations. For example, incidents with a behaviour type of actual or attempted assault.

The Notification Alert advises service centre staff of the associated risk if the customer presents in their workplace. It can be triggered with or without an image of the customer.

Where to go for processing help

- Staff can get help with CIMS and CIRT processing from the Customer Aggression Network (CANOC). See Resources for their contact details.
- For staff working with Child Support customers, see Personalised Services.

The Resources page contains:

- tables demonstrating service channel restrictions
- Safety Alert Decision Note
- customer aggression SMS
- Managed Service Plan (MSP) letter templates
- letter and text templates and guidelines
- DEMC messages user guide
- contact details
- intranet links
- Services Australia website

Related links

Customer aggression Prevention and management

Customer aggression Response

Customer aggression Managed Service Plan (MSP)

Managed Service Plan (MSP) Implementing

Managed Service Plan (MSP) Customer not complying

Managed Service Plan (MSP) Reviewing

Managed Service Plan (MSP) - Customer service delivered through a One Main Contact (OMC)

Managed Service Plan (MSP) - One-off variation

Notification Alert

Accessing and using the Customer Incident Management System (CIMS)

Family and domestic violence

Identifying customer vulnerability and risk issues

Providing services to customers with disabilities

Using the National Relay Service (NRS)

Documenting Child Support information

Nominee arrangements under Income Management

Reviewing nominee arrangements

Person Permitted to Enquire (PPE) or Update (PPU) authority

Centrelink letters online and Electronic Messaging

Sensitive Information Indicators in the CDMS

Process

This page contains the process staff follow to guide their decision making when considering proposing and approving a Managed Service Plan (MSP) and the process to propose and record an MSP.

On this page:

Requesting removal of a Note, Managed Service Plan (MSP) or safety alert record for CIMS

Proposing and recording an MSP for Medicare Public customers

Proposing and recording an MSP for Medicare Provider customers

Proposing and recording an MSP for Personalised Services for Child Support customers

Considering and approving an MSP

Review and update a Centrelink MSP in Cuba and CDMS

Before proposing an MSP - Centrelink, Medicare and Child Support

Table 1

Step	Action
1	**Principles of decision making in proposing an MSP** + Read more ... If an incident of customer aggression or counterproductive behaviour has occurred, see Issuing warnings to customers in response to customer aggression or counterproductive behaviour. Consider if a warning should be issued rather than proposing a Managed Service Plan (MSP). A warning is not appropriate following a serious incident of aggression. When proposing an MSP, consider the customer's individual circumstances and requirements of the individual. Take into account all available information. A proposal for implementing an MSP should be completed as soon as possible (within 48 hours) in order to keep staff safe. Principles to apply while considering the proposal are below. **Customer contribution:** • Where possible, give the customer the opportunity to contribute • Use objective decision making - make sure there is no bias. For example, it may not be appropriate for a person affected by the initial incident to be involved in the process • Evidence-based decision making - gather evidence to support the decision. For example, a decision without personal opinion or assumptions • Address matters that remain unresolved. For example, discuss the customer's right to request a review with genuine consideration and through the agency's complaint process • Underlying triggers - consider the customer’s situation and how it may be addressed through MSP servicing strategies. For example, whether the customer is transient, homeless, has severe mental health issues, is experiencing domestic violence • Consider how the restrictions may compound vulnerabilities for the customer **For referrals from:** • Health Services Delivery Division (HSDD), Escalated or External Complaints, Media Branch, National Restricted Access Team (NRAT), Senior Executives, Smart Centres, Social Work Services or Intelligence and Investigations, or where the customer is identified as high risk through proactive data analysis, go to Step 13 • **Centrelink** staff and HSDD CANOC, go to Step 2 • **Child Support** staff, go to Step 3
2	**Who is involved in proposing an MSP** + Read more ... It is important that appropriately skilled staff be involved in the proposal. By convening a Local or Zone Assessment Panel, contributions can be sought from: • specialist staff. For example, a social worker or psychologist • representatives from other service delivery brands if the MSP relates to a mutual customer. For example, HSDD CANOC or Child Support Team Leaders or Managers • leadership from the affected site (service centre or Smart Centre) • the relevant Customer Aggression Network Operational Contact, (Service Zone, Smarts, HSDD or other business areas)

	• if the incident/s involved partner agency staff, a representative from that partner agency • a representative from the Customer Aggression Prevention Team (CAPT) • Legal Services • Personalised Services Resources has links to Intranet pages to Customer Aggression Prevention, Customer Aggression Network Operational Contact (CANOC) contact details (Service Zone, Smarts and HSDD). See Customer aggression Managed Service Plan (MSP) for Local, Zone and Assessment Panel structures.
3	**Contact customer before proposing the MSP** + Read more ... Contacting the customer by telephone is the preferred method where possible, before proposing an MSP. This allows for timely contact and gives the customer the opportunity to give details of their circumstances and additional relevant information. There are limited circumstances where it is not appropriate to contact a customer. Wherever possible contact the customer's Power of Attorney, nominee or person permitted to enquire or update (PPE or PPU) where a decision is made not to contact the customer directly. Centrelink - Nominees, PPE or PPU: the MSP proposal process provides an opportunity to review existing voluntary arrangements. An example is when family and domestic violence are a concern between the customer and the authorised person. For more information, see Reviewing nominee arrangements. Contacting the customer gives them a chance to give information that may explain their behaviour and any additional relevant information. For example, if they have a disability or medical condition, they may need to discuss how they may be adversely affected by the proposal. This helps inform MSP strategies and gives the customer the opportunity to be heard. Services Australia expectations and responsibilities should always be discussed in this contact. If an incident of customer aggression or counterproductive behaviour occurs: • see Customer aggression - Post incident contact and • consider if a warning should be issued instead of proposing an MSP. A warning is not appropriate following a serious incident of aggression If a Provisional MSP is being considered, it may not be appropriate or possible to contact the customer. Staff and site safety takes precedence. For information about Provisional MSPs, see Customer aggression - Managed Service Plan.
4	**Consider all relevant information when proposing the MSP** + Read more ... Consider all relevant information in the MSP proposal, including information: • provided by the customer/nominee • recorded by the agency, such as complaints or adverse decisions • external organisations, such as providers, police, or community organisations • provided by staff in relation to any incident or pattern of behaviour **Note:** access call recordings if appropriate. See Call recording - information and access s47E(d)

s 22 s 22

	s47E(d)
5	**Consider the timeframe for the MSP** + Read more ... The timeframe for the MSP needs to be appropriate to the circumstances and the level of risk to the agency and customer. After an incident of customer aggression, a Provisional MSP of 24 hours to 10 business days gives the agency time to assess future risk. This also allows the customer time to consider their actions and responsibilities when dealing with the agency. When implementing a Provisional MSP for a period including public holidays, CIMS will not identify and take into account public holidays. This may limit the number of working days available to assess and implement a longer term MSP. Consider the impact of public holidays when assessing longer term MSPs. During a Provisional MSP the agency may determine that a longer period is required to make sure the risks posed by the customer are mitigated, their issues resolved and needs met and to give a chance for any servicing strategies to take effect. Consider the following in relation to the length of the proposed MSP: **Provisional MSP (Centrelink and Medicare Public only)** • 1 - 5 business days for low severity and low future risk of further incidents of aggression • 6 - 10 days for serious, moderate or multiple incidents of aggression to allow time to make a decision about a longer term MSP A Provisional MSP allows time for the following to take effect: **Service recovery** Contact the customer to: • discuss the incident and hear their side of the story • discuss behavioural expectations • identify and follow up on any service issues, such as payment or decision delays, complaints about staff behaviour • offer options such as a referral, lodge a complaint/appeal, claim an alternative payment, etc. **Assess risk** • Vulnerabilities, complex issues, disabilities and medical conditions or other barriers • Customer's responses and behaviour during post incident contact • Include specialist staff in a Local Assessment Panel (LAP) or Zone Assessment Panel (ZAP) **Take action** • Determine appropriate servicing strategies that support the customer and keep staff safe, such as referrals, service channel restrictions, Personalised Services management • Select a One Main Contact (OMC) and back up OMC for the customer • Obtain delegate approval for the long term MSP **Long term MSP**

	11 or more business days is appropriate where there are ongoing risks to the safety of staff, or the agency needs to provide an OMC to prevent further triggers of aggression. Where the trigger for aggression has not been resolved, or there is a significant likelihood of more aggression, a longer term MSP would be appropriate. See Customer aggression Managed Service Plan (MSP) for more information about the types of MSP and timeframes.
6	**Consider the end date of the proposed MSP when using CIMS/CIRT** + Read more ... The MSP ends automatically when the recorded end date is reached. For longer term MSPs (11 days or more), carefully consider the end date to make sure the agency has adequate opportunity from the initiation of the automatic review email to the end date (28 days) to make an informed decision. For example, consider any public holidays or other events that may affect the ability to appropriately review the MSP. **Note:** a review email does not generate for Provisional MSPs (1 to 10 business days).
7	**Determine the type of MSP** + Read more ... MSPs are implemented: • with a restriction to service channels: ◦ following an incident of customer aggression or counterproductive behaviour including where the behaviour is directed at another customer ◦ a risk prevention strategy for customers who may pose a future risk to staff safety • to assist a customer: ◦ who has identified vulnerabilities or barriers ◦ an early intervention or tailored services strategy where a customer has escalated contact through Escalated or External Complaints, Media Branch, National Restricted Access Team (NRAT), Senior Executives, Smart Centres, Social Work Services or Intelligence and Investigations, or where the customer is identified as high risk through proactive data analysis For more information, see Customer aggression - Managed Service Plan.
8	**Consider service channel restrictions** + Read more ... The agency may place full or partial service channel restrictions on each of the primary service channels for customer contact as part of an MSP. If a channel is available, it means that it is fully available for the customer to access services normally through that channel. Consider the following factors when proposing a service channel restrictions for a customer: s 47E(d) For Child Support customers, service channel restrictions can only be considered after a referral to Personalised Services. For more information, see Referring customers to and handling enquiries and correspondence for Personalised Services. Resources has a table demonstrating the types and levels of service channel restriction.
9	**Consider a safety alert** + Read more ... Where an incident of customer aggression is recorded with a behaviour type of actual assault, attempted assault or actual stalking, a safety alert must be considered. s47E(d) The decision to implement a safety alert is separate to the decision to implement an MSP. The customer must, however, have an active MSP for a safety alert to be applied.

	For a long term MSP, a safety alert approved decision maker should consider recommendations from a LAP or ZAP to help inform their decision.
10	**Consider a Notification Alert** + Read more ... A Notification Alert **must be considered** when an incident of customer aggression is recorded with a behaviour type of: • actual assault • attempted assault, or • stalking When the customer attends a Service Centre, a Notification Alert appears in the s47E(d) , within the s47E(d) The Notification Alert displays customer details including their name and CRN. It has a link to the customer's MSP and an option to view an image of the customer if one is available. The customer must have an active MSP for a Notification Alert to be applied. For more information see Notification Alert.
11	**Consider servicing strategies** + Read more ... Use indicators of vulnerability and risk issues to assess if it is appropriate to consult with or refer the customer to available resources, external service providers or agency specialist staff. Make a referral to the appropriate area if the customer requires specialised assistance. The Family and Domestic Violence Support (FDVSM) Model supports staff to identify customers affected by family and domestic violence. Servicing strategies can include: • Internal referrals, such as: 　○ Community Engagement Officers (CEO) 　○ Indigenous Services (ISO) 　○ Multicultural Services, including interpreter services 　○ Social work services 　○ Employment Services Assessment (ESAt) or Job Capacity Assessment (JCA) 　○ Incarcerated Customer Services • External referrals, such as: 　○ anger management counselling 　○ financial planning 　○ Workforce Australia Employment Services Provider 　○ housing/accommodation provider 　○ Legal Aid 　○ welfare agency • Other strategies, such as: 　○ appointing a nominee or person permitted to enquire (PPE) 　○ weekly payments 　○ using self service and digital services 　○ assessing eligibility of other payment types 　○ informing and educating customers of specialist services available for use, such as interpreter services 　○ using accessibility services, such as interpreter services or National Relay Service (NRS) 　○ Email redirection 　○ Telstra inbound call customisation All servicing strategies recorded in CIMS start with a status of 'Not Started' and must be updated to reflect the progress of the strategy. The servicing strategy will require status progression updates as follows: • Not required - used in mandatory strategies where it has been identified that a customer is not a shared customer of the other service brand, or where the MSP was implemented prior to 1 July 2022 • For non-mandatory strategies this outcome confirms that the strategy no longer suits the customer's circumstances • In progress - confirms the item is in progress and requires ongoing attention • Completed - used where the strategy has been completed throughout the period of the MSP

	For mandatory strategies, a status of completed reflects that the customer is a shared customer of the other service brand and the core system has been updated with the MSP details. Is call customisation being considered? - **Yes**, go to Step 12 - **No**, go to Step 13 If an email redirection is being considered, see Managed Service Plan (MSP) Email redirection.
12	s 47E(d)
13	**Consider options for customer management** + Read more ... For Centrelink customers: - MSP proposal, see Table 2 - Referral to Personalised Services, go to Step 13 For Medicare Public customers: - see Table 4 For Medicare Provider customers:

	• see Table 5 For Child Support customers: • see Table 6 For shared premises sites, go to Step 14.
14	**Personalised Services - referrals from Centrelink and Medicare** + Read more ... Referrals from these areas are made **directly to PS**: • Escalated and External complaints • Media Branch • National Restricted Access Team (NRAT) • Senior Executives • Smart Centres • Social Work Services • Intelligence and Investigations, or • HSDD CANOC PS accepts these referrals and assesses the customer aggression risk and appropriate ongoing case management. **Direct referrals** are only for customers who have **no**: • current restrictions on accessing agency services • aggression incidents in the last 12 months within the face to face environment • current case management by Service Zones • identified risk to face to face To make a direct referral to PS, see Referring customers to and handling enquiries and correspondence for Personalised Services. Procedure ends here **Referrals to PS from all other areas are assessed on their suitability for PS case Management.** For information about: • Personalised Services team, including the service they offer and how to make a referral, see Personalised Services • making a referral to PS, see Referring customers to and handling enquiries and correspondence for Personalised Services
15	**Shared premises** + Read more ... **Joint MSP with service channel restrictions** Where a mutual customer is involved in an incident, Services Australia and partner agency staff collaborate to determine impacts on servicing and proposed contact points. Where service channel restrictions are being implemented, the owning agency should communicate the initial advice by phone and in writing (a co-signed letter must be issued). Include the following information when communicating with the customer by phone or in writing: • Details about future servicing and the agreed access channel/s to partner agency services available on site. For example NDIA, ATO or DVA • Where each agency appoints a One Main Contact (OMC)/Personalised Services Service Officer (PSSO), clearly explain how the customer can contact them A copy of the MSP implementation letter should be retained by both Services Australia and the partner agency. Services Australia and the partner agency staff must record any outcome impacting service on their approved customer management system/record. **Partner agency MSP with service channel restrictions**

	Where the partner agency intends to implement a restriction while Services Australia does not, the restriction does not apply to other on site services where Services Australia is the premises leaseholder. Partner agency staff must record any outcome affecting their service on their approved customer management system/record. The relevant CANOC, Customer Aggression Prevention Team (CAPT) and Face to Face Partnerships team can be contacted for support and advice. For Centrelink, see Table 2.
16	**MSP proposals for staff members with a private protection order (including family violence orders) against a person who is also a customer** + Read more ... **Disclosure and risk assessment** In some cases, a staff member may tell the agency that they hold a private protection order against a customer. They may ask for support to make sure they are protected. When this happens, the agency should conduct a risk assessment in consultation with the protected person, Security Branch, and relevant business areas. The risk assessment will consider what steps the agency can take to support the staff member. **Privacy and confidentiality** A possible outcome of the risk assessment is that the agency will take a proactive approach. If this is the case, the agency must manage the situation carefully to **avoid**: • disclosing any personal information about the protected person • including a requirement that may breach the order. s 47E(d) Disclosing the staff member's protection order without their consent may: • breach the Privacy Act • increase risk to the safety of anyone in the workplace. An MSP with service channel restrictions may be considered. This depends on the individual circumstances and the staff member's preferences. s 47E(d) It may be appropriate to modify the standard MSP letter to tell the customer that it will help them to comply with their protection order, rather than as a consequence of their behaviour. Contact CAPT for help with MSP letter templates. For more information about supporting staff, see Customer aggression - Staff Support

Proposing and recording an MSP for Centrelink customers

Table 2: the process to use when recording either a provisional or long-term MSP.

Step	Action
1	**Who can record and manage an MSP for Centrelink customers** + Read more ... Staff with the CIMS Manager and Delegate Security role can: • propose an MSP with or without service channel restrictions • create a provisional MSP, including a safety alert if relevant. It will become active once saved and submitted Staff with the CIMS Delegate Security role can:

- activate a long term MSP by approving proposed channel restrictions, and a safety alert if relevant

Note: MSPs can be released under the Freedom of Information Act. All information in CIMS must be factual, use exact quotes (verbatim), and cannot include personal commentary or opinion.

Personalised Services (PS) will manage the MSP proposal when the following criteria apply:

- PS received the referral directly from:
  - Escalated or External Complaints
  - Media Branch
  - National Restricted Access Team (NRAT)
  - Senior Executives
  - Smart Centres
  - Social Work Services
  - Intelligence and Investigations
- The customer has no current restrictions on accessing agency services
- The customer hasn't been involved in aggression incidents in the last 12 months in a face to face environment
- There is no current case management by the Service Zone

For all other situations, PS will liaise with the relevant Zone.

2 **Create the MSP in CIMS** + Read more ...

Staff can create an MSP from:

- the incident record
- a Provisional MSP
- the customer's record in Process Direct or Customer First
- the CIMS Launchpad

Create MSP from an incident record + Read more ...

Staff can create an MSP from an incident record if both of the following apply:

- It is submitted or finalised
- There is a Customer Reference Number (CRN) recorded on the s 47E(d) page, under s 47E(d)

s 47E(d)

Create a long-term MSP from a Provisional MSP + Read more ...

A review should be completed on an active Provisional MSP. As part of the review process, staff may decide to:

- return the customer to mainstream service on approval
- return the customer to mainstream service the day after their MSP ends
- implement a long term MSP immediately after the current Provisional MSP ends (extend MSP)
- replace the current Provisional MSP before the end date with a long term MSP

To initiate the long term MSP from an active Provisional MSP, s 47E(d) .

Create an MSP from a customer's record in Process Direct + Read more ...

If the customer record has an active MSP, use the review process instead. See Managed Service Plan (MSP) - Reviewing.

If the customer record does not have an active MSP, access the customer's s 47E(d) s 47E(d)

s 47E(d)

The s 47E(d) shows:

	• any current MSP that is already in place for either Services Australia or the Department of Employment and Workplace Relations • if any previous incidents of aggression have been recorded on this CRN s 47E(d) **Create an MSP from a customer's record in Customer First** + Read more ... If the customer record has an active MSP, use the review process instead. See [Managed Service Plan (MSP) _ Reviewing.]() If the customer record does not have an Active MSP in place s 47E(d) s 47E(d)
3	**Set up the MSP record** + Read more ... s 47E(d)
4	**Complete the** s 47E(d) **page** + Read more ... s 47E(d) **MSP Details** + Read more ... Complete the following mandatory fields.

s 47E(d)

The start date depends on:

- the date of an incident
- the day a current MSP ends
- the date that changes must be made to existing servicing restrictions

Restrictions + Read more ...

This section records the proposed Service Channel Restrictions recommended during a Local Assessment Panel/Zone Assessment Panel meeting.

Each channel's restrictions apply across all service brands, unless the note describes different levels of access amongst the service brands. Consider all three channels: face to face, phone, and writing.

s 47E(d)

Each restriction can have a note. s 47E(d)

The note should discuss how the risks against each brand have been considered. A partial restriction **must** have a note to explain the restrictions.

Select s 47E(d) at the right of each row to read a note.

Each restriction has a status. The status auto-populates and will change from **Draft** to **Approved** once the overall MSP becomes active.

To delete a restriction, s 47E(d)

5 **Complete the** s 47E(d) **page (long-term MSPs only)** + Read more ...

The s 47E(d) page only appears if the MSP is a long-term MSP. It has 3 sections:

s 47E(d)

Personalised Services Referrals + Read more ...

To add a referral for Personalised Services (PS), select s 47E(d)
s 47E(d)

Personalised Services reasons include the following:

- **Behavioural**: for customers with a tendency or history of using aggression, or making threats of aggression
- **Complexity**: for customers who need to be managed by a technically skilled staff member, along with social work services
- **Privacy Breach:** for customers who may have experienced a breach of privacy

- **Sensitivity**: to contain the management of the customer to prevent multiple handling and to ensure a whole of agency response
- **Vulnerability**: for customers who need priority treatment and management. An example could be a customer who is experiencing vulnerability, but their situation doesn't meet the DSP requirements
- **Vexatious**: the customer continually or persistently uses unreasonable behaviour that hinders our ability to provide service. The customer's behaviour may make it difficult to work out what the genuine issue is

Servicing Strategies + Read more ...

Servicing strategies are the action items of an MSP. The OMC/PSSO will update these throughout the active MSP period. Choose strategies that address the barriers and vulnerabilities that the customer experiences.

Long term MSPs contain two mandatory servicing strategies]

- Review and update MSP details in CUBA
- Review and update MSP details in CDMS

Both servicing strategies start with a progress status of Not Started. They should start as soon as the MSP is approved to make sure that service channel restrictions are followed across all service brands.

To add more servicing strategies, select **+** s 47E(d)
Select the appropriate options from these menus. To remove one s 47E(d)

Specialist Consultations + Read more ...

A specialist may be consulted before or during an MSP. Record the date and details of these consultations in this section.

To add a consultation, select the s 47E(d)

Specialist referrals s 47E(d) include:

- Social Worker
- Forensic Psychologist
- Assessment Services
- Legal Services
- Customer Aggression Prevention Team
- Multicultural Services
- Indigenous Services
- Incarcerated Customer Services Team
- Community Engagement Officer Network
- Protective Services
- Smart Centre Critical Response Team
- Complaints
- Referral to ACER team

6 **Complete the Notes page** + Read more ...

The Notes page is for adding free text notes to the record. The header shows the number of notes on a record.

All MSPs must include a **Rationale for decision** note. Use the s 47E(d) button to create this note.

As a minimum, the note must contain:

- a rationale for the length of the MSP
- a brief summary of the behaviours or vulnerabilities that led to recommending an MSP
- a description of the vulnerabilities the customer experiences, and how the servicing strategies aim to address these
- an expected completion date for each servicing strategy
- a description of the ongoing risk the customer poses to staff in each service brand
- the reasons for deciding on the OMC/PSSOs chosen to support the customer

After filling in the note contents, select s 47E(d)

	s 47E(d) All free text notes recorded in an MSP are subject to Freedom of Information (FOI) Act provisions. See Freedom of Information (FOI) for further information. See Resources page in Accessing and using the Customer Incident Management System (CIMS) for MSP note types and examples, including the rationale for decision. After an MSP record has been saved or submitted, notes saved to the s 47E(d) page cannot be edited. See Table 3 for how to ask for removal.
7	**Complete the** s 47E(d) **page** + Read more ... The s 47E(d) page has 2 sections: - Related Incidents & MSPs - Internal Communications **Related Incidents and MSPs** If the MSP was created from an incident or a Provisional MSP, CIMS will automatically fill in the link to the related records. If a relevant MSP or incident was not automatically added, select s 47E(d) **Internal Communications** This section shows any emails sent from CIMS. See Resources page in Accessing and using the Customer Incident Management System (CIMS) for a guide to CIMS emails. SMS messages are not automatically recorded in this section. Add a note to the MSP to record these. See Managed Service Plan (MSP) - Implementing.
8	**Complete the** s 47E(d) **page** + Read more ... The s 47E(d) page records the details of staff members implementing, approving, or taking responsibility for the MSP. s 47E(d)

	s 47E(d)
9	**Save the MSP and attach the MSP letter** + Read more ... The mandatory fields on the following 4 pages must be complete before an MSP can be saved: s 47E(d) If the MSP is a long-term MSP, the s 47E(d) page must also be complete. Once these are complete, save the MSP. After saving the MSP, the MSP gets an ID number, and the s 47E(d) page becomes available. Go to the s 47E(d) page and attach the MSP letter. The letter must: - describe the behaviour of the customer - describe any other relevant considerations taken into account in making the decision - explain the customer's ongoing access to the agency's services - discuss the customer's right to request a review of the MSP - Include the relevant signature block. Do not record exact (verbatim) quotes of what the customer said in the letter. For help with the letter, contact the Customer Aggression Prevention Team (CAPT). During the approval process, the approver will review this draft. Make sure that it is clearly described as the draft version, such as s47E(d) See Resources for letter templates and guidelines. If a document has been uploaded to a CIMS record incorrectly, see Removing a digital image from customer records. If a safety alert is being considered as part of the MSP, see Table 3.
10	**Check and submit the MSP for approval** + Read more ... Once all the mandatory details are complete, staff can save it as a draft or submit it to an approver. s 47E(d) Select s47E(d) and check the header before leaving the record.

Adding or approving a safety alert for Centrelink customers

Table 3

Step	Action
1	**Proposing a safety alert for Centrelink customers** + Read more ... Staff with the CIMS Manager or CIMS Delegate Security role can edit MSPs to: - propose a safety alert

	- create a safety alert within a provisional MSP. It will become active once saved and approved - select Undo to restore safety alert status to inactive **Note:** this can only occur in MSP Draft status When a safety alert is proposed, a MSP Safety Alert Proposal email notification is automatically sent from CIMS to the approved decision maker for action.
2	**Who can approve a safety alert** + Read more ... The approved decision maker for a safety alert is the same as the MSP decision maker (based on the MSP type and timeframe). For a provisional MSP, staff who hold the CIMS Manager role can approve or reject the safety alert to avoid delay. CIMS Delegate Security role or further approval is not required. Staff with the CIMS Delegate Security role can: - approve all safety alerts - approve the removal of, or reject a proposed safety alert Where an incident meets the criteria, a safety alert needs to be considered as soon as practicable. An approved decision maker can provide verbal approval to activate a safety alert. If this occurs a staff member with the CIMS Delegate access can activate the safety alert on behalf of the approved decision maker. To implement a safety alert for an **existing MSP with a change to servicing restrictions**, a staff member with CIMS Manager or CIMS Delegate access must review the MSP and add the safety alert. See Table 1 in Managed Service Plan (MSP) – Reviewing To create a safety alert, go to Step 3 To approve or reject a safety alert, go to Step 6
3	**Create the safety alert in CIMS** + Read more ... A safety alert can be included when: - creating a new (provisional) MSP, or - editing a draft, active, or existing long term MSP Create a safety alert: - If the MSP is: s 47E(d) If the safety alert is being proposed inside: - a provisional MSP, go to Step 4 - a draft, active or long term existing MSP, go to Step 5
4	**The MSP is provisional** + Read more ... To approve a provisional MSP: s 47E(d)

	Procedure ends here
5	**The MSP is draft, submitted or active** + Read more ... The safety alert must be approved by a staff member with CIMS Delegate access. Staff with the CIMS Delegate access approve as the approved decision maker, or on behalf of the approved decision maker. • To approve a safety alert, go to Step 6 • To send a proposed safety alert for approval: • s 47E(d) • • Procedure ends here
6	**Approving or Rejecting the Safety Alert** + Read more ... To approve or reject a safety alert: s 47E(d)

Requesting removal of a Note, Managed Service Plan (MSP) or safety alert record for CIMS

Table 4: this table describes how staff can request the Customer Aggression Prevention Team (CAPT) to remove incorrectly recorded information from the Customer Incident Management System (CIMS).

Step	Action
1	**Reasons a CIMS Note can be deleted** + Read more ... A note recorded in the Customer Incident Management System (CIMS) can be considered for deletion when: • the note has information which could lead to or be considered a breach of privacy for a staff member or customer. For example, staff member's first and surname and/or location • the note was recorded on the wrong customer's record • judgemental language or misleading information has been included After the note is deleted, the s47E(d) will continue to display the note type, author and creation date. The deleted note text will remain in the background data of the CIMS tool. **Note:** removal of a CIMS note will result in the note text remaining in the CIMS database with only the note type, author and creation date being displayed in the s47E(d) .

2	**Request deletion of a CIMS note** + Read more ... Email a request to remove the note to Customer Aggression Prevention Team (CAPT). Include the: • CIMS MSP • customer name and/or reference number • note type, logon who created the note (created by), date and time created • brief explanation for the deletion request
3	**Reasons a CIMS record can be removed** + Read more ... An entry in the Customer Incident Management System (CIMS) may be considered for removal (excluded from reporting) when the MSP or incident of customer aggression or counterproductive behaviour was: • incorrectly recorded, for example a duplicate record has been created • recorded on the wrong customer record
4	**Request removal of a CIMS record, including safety alert** + Read more ... Email a request to remove the record to the Customer Aggression Prevention Team (CAPT). In the email include the: • CIMS MSP ID • customer name and reference number • details explaining the reason for the request of removal CAPT will respond to the requesting officer on completion of the removal action. See Removing a digital image from customer records to request any documents uploaded to the MSP record to be deleted from the customer's record. **Note:** CIMS automatically notifies the Department of Employment and Workplace Relations (DEWR) when an Incident record is removed from CIMS (if DEWR were advised of the Incident record when it was recorded).

Proposing and recording an MSP for Medicare Public customers

Table 5

Step	Action
1	**Proposing an MSP for a Medicare Public Customer** + Read more ... HSDD MSPs implemented following a CIRT incident are recorded as Proactive MSPs with restrictions in CIMS. When making a proposal or recommendation for an MSP, the s 47E(d) should provide the following information to the relevant CANOC: • Details of the customer - first and last name, date of birth, current address • Details of any vulnerabilities or barriers • CIRT or CIMS reference number - containing an accurate description of the incident • Any other action taken – referral to a social worker, police contact, s47E(d) , site closure • Details of post incident actions, see Customer aggression - Post incident contact • Rationale for implementing the MSP including the MSP duration and how the customer should contact the agency and the outcomes we would like to assist the customer with **Medicare Telephony (Smart Centre)** The Line Manager/Team Leader should make a recommendation to propose an MSP to the Health Services Delivery Division (HSDD) CANOC. • HSDD CANOC will assess the incident and refer to the Zone CANOC for MSP implementation or action. When there: ○ is a risk to face-to-face services ○ are previous incidents of aggression in face to face within the last 12 months ○ are incidents currently managed by the zone

	- In all other cases, the HSDD CANOC will complete the Referral to Personalised Services macro and liaise with Personalised Services to implement and manage the MSP For direct referrals received by PS from HSDD CANOC, PS will create and manage the MSP proposal in CIMS where the customer meets the following criteria: - No current restriction(s) on accessing agency services - No aggression incidents in the last 12 months within the face to face environment - No current case management by the Service Zone **Note:** if the Line Manager / Team Leader identifies an immediate risk to face to face services and HSDD CANOC is not available, the Line Manager is to contact the local Zone CANOC or Service Centre Manager. **Medicare Face to face (Service Centre)** - The Zone CANOC or s 47E(d) will record the MSP proposal in CIMS - The HSDD CANOC is to be notified of any MSP implemented for a Medicare Customer Resources page has CANOC contact details. When developing MSP proposals staff may seek advice from Customer Aggression Prevention Team (CAPT)
2	**Recording MSP proposals for Medicare Public customers in CIMS** + Read more ... HSDD MSPs implemented following a CIRT incident are recorded as Proactive MSPs with restrictions in CIMS. Record all information contributing to the decision to propose the MSP in the 'rationale for decision' note in the MSP, including: - CIMS Incident number/s (if applicable) - CIRT Incident number/s - duration of the MSP and why - any service channel restrictions and why - service strategies that will be put in place and why Record the proposed MSP in CDMS as a Sensitive Indicator, see Step 5. If the CANOC cannot access CDMS, provide details to the Team Leader or Manager.
3	**Draft MSP letter** + Read more ... Attach a draft of the relevant MSP letter. The letter must: - describe the behaviour of the customer - describe any other relevant considerations taken into account in making the decision - explain the customer's ongoing access to the agency's services - outline the customer's right to request a review of the MSP - include the relevant signature block **Verbatim quotes** Do not record exact (verbatim) quotes in the letter. For help with the letter, contact the Customer Aggression Prevention Team (CAPT). During the approval process, the approver will review the draft letter. Make sure that this letter is clearly described as the draft version, such as s47E(d) See Resources for letter templates and guidelines.
4	**Submit MSP proposal** + Read more ... The proposed proactive MSP must be approved by a delegated Approver if it has a duration of 11 business days or longer and includes service channel restrictions. **Does the proposed MSP include service channel restrictions and have a duration of 11 business days or longer?** - **Yes**, submit the proposal in CIMS to commence the approval process. See Table 7

	• **No**, the MSP can be implemented immediately. See Implementing a Managed Service Plan
5	**Reference MSP details in CDMS as a Sensitive Information Indicator** + Read more ... **MSP details are recorded in CDMS as a Sensitive Information Indicator with the following:** • Category: s47E(d) • Indicator **Type:** Full or Partial service restrictions The indicator triggers a **Sensitive Information alert** when staff access the record. Staff can view the indicator details from the s47E(d) Once the MSP end date recorded in the indicator is reached, the indicator: • no longer triggers the Sensitive Information alert • does not display in the s47E(d) • can only be viewed in the s47E(d) in s47E(d) Staff can view the history of amended and end dated indicators in the s 47E(d) s 47E(d) To record a **Sensitive Information** Indicator, see Adding or amending Service Indicators. For issues relating to CDMS access, liaise with the CAPT or HSDD CANOC.

Proposing and recording an MSP for Medicare Provider customers

Table 6

Step	Action
1	**Proposing an MSP for a Medicare Provider Customer** + Read more ... An MSP enables servicing Restrictions and/or Servicing Strategies to be applied for a period of between 6 business days and 12 months. Where an MSP is proposed, the s 47E(d) or Zone CANOC will liaise with the Health Services Delivery Division (HSDD) CANOC and provide the following information: • Details of the customer - first and last name, all available reference numbers, address • Customer Incident Recording Tool (CIRT) reference number so an accurate description of the incident can be accessed • Any other action taken – referral to a social worker, police contact, s47E(d) , site closure • Details of post incident actions, see Customer aggression - Post incident contact • Rationale for implementing the MSP including the MSP duration and how the customer should contact the agency as per MSP template When developing MSP proposals staff may seek advice from Customer Aggression Prevention Team (CAPT). HSDD CANOC representatives should go to Step 2
2	**Recording an MSP for a Medicare Provider Customer** + Read more ... **Action required by HSDD CANOC** Management of the proposed MSP: • Make sure details of the incident have been recorded in CIRT as per the details provided by the Team Leader or Manager, follow the steps in Reporting, recording and escalating incidents of customer aggression • Record a proposed MSP in the s 47E(d) • s 47E(d) • and decide if it will be Approved or Withdrawn • Review all available information of the incident

s 22

s 22

	Enter all available information in the CIRT MSP: s 47E(d)

3	**Draft MSP letter** + Read more ... **Action required by HSDD CANOCs** Attach the relevant draft MSP letter to the s 47E(d) The letter must: - describe the behaviour of the customer - describe any other relevant considerations taken into account in making the decision - explain the customer's ongoing access to the agency's services - outline the customer's right to request a review of the MSP - include the relevant signature block **Verbatim quotes** Do not record exact (verbatim) quotes in the letter. For help with the letter, contact the Customer Aggression Prevention Team (CAPT). During the approval process, the approver will review the draft letter. Make sure that this letter is clearly described as the draft version, such as s47E(d) See Resources for letter templates and guidelines.

Proposing and recording an MSP for Personalised Services for Child Support customers

Table 7

Step	Action
1	**Personalised Services referral Child Support customers** + Read more ... Child Support Personalised Services manages the process for Child Support customers who: - display unreasonable conduct and - restricting service options is recommended For referral criteria for Personalised Services, see Customer referral guidelines.
2	**Proposing an MSP for a Child Support customer** + Read more ... Record a proactive MSP with restrictions in CIMS and the Child Support Personalised Services Customer Management Plan (CMP) in Cuba, if the customer poses a risk to other service brands **when 1 or more** of the below criteria are met: - Has had multiple, moderate or serious incidents of customer aggression after commencing PS management - Has service restrictions preventing attendance at a service centre or from calling another Services Australia phone service - Has advised they will contact the agency outside the PS phone channel, including another phone service or in person A MSP can also be implemented proactively when a customer needs to be provided with additional support to access the agency's services. If a PS Service Officer (PSSO) recommends a CIMS MSP, a PS Service Manager (PS SM) provides endorsement and rationale to the Child Support Assessment Panel. The PS Child Support Program Support Manager (PSM) should liaise with the zone CANOC to record the MSP. See Resources for CANOC contact details. The PSM provides the following information to the CANOC: - CIMS Incident number/s (if applicable) - CIRT Incident number/s - Details of the customer (name, DOB, address)

	- Post incident actions, Issuing warnings to customers in response to customer aggression or counterproductive behaviour - Rationale for implementing the MSP (including the MSP duration and how the customer should contact the agency) - PSM endorsement Staff may seek advice from Customer Aggression Prevention Team (CAPT). - CANOC representative, go to Step 3 - PSSO, go to Step 4
3	**CANOC** + Read more ... The CANOC must: - refer to the incident's details recorded in CIMS/CIRT by the Child Support PSSO - discuss with the Child Support PS PSM the appropriate MSP options as endorsed by PS SM per Table 1, Factors to consider before proposing a Managed Service Plan - propose and record an MSP in CIMS as per Table 2 including recording the MSP details in Medicare CDMS. Record MSP details as a Sensitive Information Indicator in CDMS, see Table 4, Step 5 - maintain regular contact with the Child Support PSSO to make sure the MSP review is conducted as per Managed Service Plan (MSP) _ Reviewing Procedure ends here.
4	**Child Support PSSO** + Read more ... Child Support PSSO must undertake the following to update the CIMS MSP in Cuba: - s47E(d) to locate details of CIMS MSP - record the date the CIMS MSP was created in the s 47E(d) box in the s 47E(d) window Resources page of Personalised Services has Table 1 - Documentation for Child Support PS s 47E(d)

Considering and approving an MSP

Table 8: how approved decision makers assess and process an MSP with restrictions.

Step	Action
1	**Receive and open the proposal** + Read more ... When an MSP of more than 10 days is submitted, CIMS will automatically email the restriction or review approver listed on the MSP's Employees Responsible page. The email contains a link to open the MSP in CIMS. The MSP will automatically email the restriction approver to notify of a submitted proposal for a safety alert. See Table 3 > Step 2

	s 47E(d)
2	**Check the** s 47E(d) **page** + Read more ... Go to the MSP's s 47E(d) page. There are 2 notes to check: • Rationale for decision • Review recommendation **Read the rationale for decision** Check the s 47E(d) note. The note should contain: • the rationale for the length of the MSP • an explanation of the proposed channel restrictions and the service brands that the channel restrictions apply to • a brief summary of the behaviours or vulnerabilities that have resulted in the recommendation to implement an MSP • a description of the customer vulnerabilities and the way servicing strategies will address these • an expected completion date for each servicing strategy • an assessment of the ongoing risk the customer poses to staff • the rationale for the OMC/PSSOs chosen to support the customer during the MSP See Resources page in Accessing and using the Customer Incident Management System (CIMS) for MSP note types and examples, including the rationale for decision. **Read the review recommendation note** Check the s 47E(d) note. It should include: • a summary of the Local or Zone Assessment Panel meeting recommendations that have been accepted, or rejected • an update on the status of any servicing strategy that has not been completed by the end of the original MSP If the MSP is an extension of an existing MSP, the previous MSP's Review recommendation note will automatically appear on this MSP's s47E(d) page. Check the Safety Alert Decision (proposal) note. See Resources page in Accessing and using the Customer Incident Management System (CIMS) for MSP note types and examples, including the rationale for decision
3	**Check service channel restrictions** s 47E(d) **page)** + Read more ... The s 47E(d) page has 3 sections: • MSP details • Restrictions, including notes about each service brand affected by the decision • Variations For more about approving a short term variation to a MSP, see Managed Service Plan (MSP) - One-off variation.
4	**Check the** s 47E(d) **page** + Read more ... The staff member who prepared the MSP should have attached a draft letter to the MSP.

	The approver should: • review the draft letter from the s 47E(d) page • upload a final copy of the letter. In the file's description, make sure to note that this letter is clearly described as the final version, such as s47E(d)
5	**Check the** s 47E(d) **pages** + Read more ... The s 47E(d) page includes details of: • any referral to Personalised Services (PS) • servicing strategies which need to be addressed during the MSP • specialist consultations completed during the development of the MSP Long term MSPs contain two mandatory servicing strategies: • Review and update MSP details in CUBA • Review and update MSP details in CDMS Both servicing strategies start with a progress status of Not Started. These servicing strategies make sure that channel restrictions are considered across all service brands and applied as required. Other servicing strategies should address the barriers and vulnerabilities that the customer experiences which can affect their return to mainstream servicing. During the MSP, staff with Manager level or above will update the strategies. Specialist consultations contribute to the risk assessment and are also recorded here, if relevant. Referrals to Personalised Services should have been finalised before sending an MSP to approve.
6	**Check the** s 47E(d) **page** + Read more ... The s 47E(d) page contains: • links to associated incidents and MSPs. If this is a proactive MSP, there may be no related incidents or MSPs yet. • a summary of CIMS-generated internal emails about the MSP.
7	**Consider, then record the decision** + Read more ... Once the approver has reviewed each of the relevant screens, they can make a decision about whether the MSP can be approved. Approvers must make sure that the MSP: • adequately addresses the risk posed by the customer • reflects the recommendations discussed in the Rationale for Decision note **Add an** s47E(d) **note** + Read more ... s 47E(d) The note should include both: • the endorsement of the recommendations • the approver's details For example: "MSP reviewed and approved by (role), (zone)" or "MSP reviewed and approved by (role), (zone) on behalf of (role), (zone)." **Approve, send back, or reject the MSP** + Read more ... If the MSP is not already in edit mode, s 47E(d) . The footer will update, and now display s 47E(d)

	s 47E(d) Any action from this menu will apply to: • any restrictions that weren't individually addressed on the s47E(d) page • the MSP overall **Approve** Approve will endorse any MSP restrictions that haven't already been approved and implement the MSP from the start date. If there are individual restrictions that should not be part of this MSP, return to the s 47E(d) page and reject them from there. **Send Back** Send Back returns the MSP with feedback about why the MSP is not approved. For example, the approver may decide that the MSP does not: • reflect the recommendations or vulnerabilities outlined in the 'Rationale for Decision' note • adequately address the risk posed by the customer Sending back an MSP means that the submitter can edit the plan and resubmit it. **Reject** Rejecting an MSP updates the record to Rejected. No more actions can be done on that record. **Save to confirm the action** + Read more ... After selecting s 47E(d) . A success message will appear. Select s 47E(d) and check the header to make sure it reflects the expected status. CIMS will now send an email to the relevant staff members to tell them about the outcome.

Review and update a Centrelink MSP in Cuba and CDMS

Table 9: Long-term MSPs have two mandatory servicing strategies, which are to review and update the MSP in Cuba and CDMS.

Step	Action
1	**Replicate an MSP in Medicare Consumer Directory Management System (CDMS)** + Read more ... Staff must reference a Centrelink MSP in CDMS whenever the customer is also a Medicare customer, and they pose a risk to Medicare staff. Staff must conduct a risk assessment to check this. **Identifying Medicare customers** s 47E(d) **Conducting a risk assessment** Areas to consider when conducting a risk assessment include whether a customer has: • accessed multiple service brands

- had multiple low, moderate or serious incidents of customer aggression in any service brand, or with Department of Employment and Workplace Relations (DEWR), in the past 12 months
- service restrictions preventing attendance at a service centre or from calling another Services Australia phone service
- has contacted the agency outside any existing service channel restrictions, or says that they intend to do that

Replicating MSP details in CDMS

Record the MSP details in CDMS as a Sensitive Information Indicator for Full or partial service restrictions. See Table 4 > Step 5.

For issues relating to CDMS access, liaise with the CAPT or HSDD CANOC.

Updating the mandatory servicing strategy in CIMS

CIMS includes a mandatory servicing strategy for long term MSPs to review and update MSP details in CDMS.

All servicing strategies recorded in CIMS start with a status of 'Not Started' and must be updated to reflect the progress of the strategy.

The available servicing strategy progress updates are:

- Not required   used where it has been identified that a customer is not a shared customer of the other service brands, or where the MSP was implemented prior to July 1 2022
- In progress   confirms the item is in progress and requires ongoing attention
- Completed - reflects that the customer is a shared customer of the other service brand and the core system has been updated with the MSP details

2 **Replicating MSPs in Child Support Cuba System** + Read more ...

Staff must reference a Centrelink MSP in Cuba whenever the customer is also a Child Support customer, and the customer poses a risk to Child Support staff. Conduct a risk assessment to check this.

Identifying Child Support customers

To check whether the customer is a mutual Child Support customer:

s 47E(d)

Conduct a risk assessment

Areas to consider when conducting a risk assessment include whether a customer:

- accesses multiple service brands, i.e. Centrelink, Medicare and Child Support
- has had multiple low or moderate or serious incidents of customer aggression, in any service brand, or Department of Employment and Workplace Relations (DEWR), within the past 12 months
- has service restrictions preventing attendance at a service centre or from calling another Services Australia phone service
- has advised they will/or has contacted the agency outside existing service channel restrictions

Referring the details to the Child Support CANOC

If the customer is identified as a mutual customer who poses a risk to Child Support, the owning Zone CANOC should email Personalised Services and provide the following:

- Details of the customer (CRN, name, DOB, address)
- MSP start date:
- MSP ID:
- MSP end date:
- OMC/PSSO/Backup Contact Officer:
- MSP Service Channel restrictions:

Child Support Personalised Services Service Officers (PSSO) reference the MSP servicing arrangement in the Cuba s47E(d) , see Table 6 > Step 4.

Updating the mandatory servicing strategy in CIMS

CIMS includes a mandatory servicing strategy for long term MSPs to review and update MSP details in CUBA

All servicing strategies recorded in CIMS start with a status of 'Not Started' and must be updated to reflect the progress of the strategy.

The available servicing strategy progress updates are:

- Not required used where it has been identified that a customer is not a shared customer of the other service brands, or where the MSP was implemented prior to July 1 2022
- In progress confirms the item is in progress and requires ongoing attention
- Completed reflects the customer is a shared customer of the other service brand and the core system has been updated with the MSP details

References

This page contains links to legislation and a description of the legal authority Services Australia uses to withdraw consent to enter Commonwealth property.

Legislation

s 22

Public Governance, Performance and Accountability Act 2013

Public Order (Protection of Persons and Property) Act 1971 (POPPPA)

Work Health and Safety Act 2011

Legal authority to withdraw consent to enter Commonwealth premises

Services Australia has a right, as the occupier of Commonwealth premises, to withdraw its consent for any person to come on to Commonwealth premises. Where a person comes on to Commonwealth premises, despite consent having been withdrawn (through the implementation of service restrictions) they are deemed to be trespassing on the premises.

The Public Order (Protection of Persons and Property) Act 1971 (POPPPA) makes it an offence to trespass on Commonwealth premises, and therefore the agency has a legal mechanism to enforce service restrictions that prevent entry into one or more of the agency's premises.

There are also broader legal mechanisms which allow the agency to manage the way in which services are delivered to people and legally support the use of MSPs and service restrictions, including:

- The chief executive powers under the Social Security (Administration) Act 1999 and Medicare Australia Act 1973 to administer the social security law and Medicare functions, and the Secretary's power to administer the Child Support legislation under the Child Support (Registration and Collection) Act 1988, which can include making incidental arrangements to support the administration of those functions (such as making arrangements to make sure the effective delivery of services by limiting interruptions caused by unreasonable customer conduct)
- Obligations under the Public Governance, Performance and Accountability Act 2013 to make sure the effective and efficient use of Commonwealth resources, for example, protecting Commonwealth property from damage
- Obligations under the Work Health and Safety Act 2011 to protect the health and safety of staff, customers, and visitors, which may necessitate restricting the way in which a person does business with the agency

Resources

Face-to-face service channel restrictions

Table 1: this table describes full and partial face to face service channel restrictions considered as part of a Managed Service Plan (MSP).

Type	Effect	Example 'free text' notes
Face-to-face - full restriction ▲ Restricted	Customer cannot attend, in person, any location where services provided by Services Australia are delivered. Under no circumstances should the customer attend in person unless a One-off servicing variation to a Managed Service Plan (MSP) is approved.	s47E(d)
Face to face partial restriction 🟧 Partially	Customer has limitations on how, when and where they may access face to face services. This includes: • Customer is directed to attend another location(i.e. can only attend at certain times or a number of times a week this is when limiting high contact), or • Customer can attend a service centre at a particular day/time (i.e. customer can attend certain sites but not others. For example, can attend a Remote Community site to see a One Main Contact (OMC) at agreed time), or • OMC to arrange an appointment before attending a service centre (i.e. must book an appointment via OMC, this is to make sure site is prepared for a visit and OMC is available). Clear risk assessment and decision making must be documented in customer's MSP in such cases	s47E(d)
Face-to-face - available ● Available	Customer has **no limitations** on how, when and where they may access face-to-face services.	No restrictions

Telephone service channel restrictions

Table 2: this table describes full and partial telephone service channel restrictions considered as part of a Managed Service Plan (MSP).

Type	Effect	Example 'free text' notes
Telephone - full restriction ▲ Restricted	Customer cannot telephone any agency telephone number. This can include One Main Contact and/or Personalised Services Officer's number.	s47E(d)
Telephone - partial restriction 🟧 Partially	Customer has limitations on how and when they are able to telephone the agency. Customer is directed to only call their One Main Contact or Personalised Services Officer.	s47E(d)
Telephone - available ● Available	Customer has **no limitations** on how to telephone any agency numbers	No restrictions

Writing service channel restrictions

Table 3: this table describes full and partial writing service channel restrictions considered as part of a Managed Service Plan (MSP).

Type	Effect	Example 'free text' notes
Writing - full restriction ▲ Restricted	Customer cannot contact the agency through any written or digital channel.	s47E(d)
Writing partial restriction 🟧 Partially	Customer has limitations on how they are able to write to the agency. This includes: • customer is directed to write to a single specific address, and/or • a restriction is placed on the customer's use of Upload documents online	s47E(d)
Writing - available ● Available	Customer has **no limitations** on how to contact the agency through any written or digital channel.	No restrictions

Safety Alert Decision Note

Table 4: this table describes what to include when adding a note for each Safety Alert status, and provides example text.

Safety Alert Status	Minimum inclusion	Example text
Safety Alert and Provisional MSP implement (approve)	• Decision maker details for verbal approval for safety alert • Confirmation of whether the safety alert criteria is met • Customer behaviour and staff safety factors taken into account • Consideration of any immediate risk the customer poses to staff and customers • Any other sources of information considered to arrive at the decision	s47E(d)
Safety Alert and Provisional MSP ends (no long-term MSP)	• Rationale for not progressing with a long-term MSP and safety alert • The actions of the customer and the well-being of employees have been carefully considered • Outcome of post incident contact with customer • Any other sources of information considered to arrive at the decision	s47E(d)

s 22	s 22	s47E(d)
Safety Alert (proposal)	• The safety alert criteria that were met • A summary of the customers behaviour that prompted the proposal Who else was involved in the recommendation to propose a Safety Alert e.g. LAP/ZAP, approved decision maker	s47E(d)
Safety Alert (approve)	• Confirmation of whether the safety alert criteria is met • Customer behaviour and staff safety factors taken into account • Consideration of any ongoing risk the customer poses to staff and customers • Any other sources of information considered to arrive at the decision	s47E(d)
Safety Alert (reject)	• Reason for the rejection of the safety alert • Actions of the customer and the well-being of employees have been carefully considered • Any other sources of information considered to arrive at the decision	s47E(d)

s 22 s 22 s47E(d)

Customer aggression SMS (Centrelink only)

- Centrelink letters online and Electronic Messaging
- Desktop (DEMC) Messages user guide
- SMS/Email Search (SMEM) screen

Customer aggression letter templates and guidelines

Letters sub-site - General Correspondence

See Customer aggression:

- Guide to Customer aggression letter templates
- Proactive MSP
- MSP Face to Face and call restriction
- MSP Write only

Macro

Referral to Personalised Services

User guide

DEMC messages

Contact details

Customer Aggression Network - Operational Contact (CANOC) role (includes relevant email addresses including Smart Centres)

Customer Aggression Prevention Team (CAPT)

Customer Response Team

Personalised Services Child Support

Personalised Services

Telephony Transformation team

Intranet links

Assessment Services: Risk Assessment Tool

Customer aggression prevention - networks and stakeholders

Intervention, Protection Orders and Apprehended Violence Orders in Australia

Smart Centres Escalations (search the intranet for this page)

Template

Agency telephony vendor inbound call customisation form

Services Australia website

Accessibility

Our service commitments

Payment and Service Finder

Training & Support

The agency's customer aggression training, the Managing Aggressive Behaviour Program (MAB Program) is mandatory for customer contact staff and their direct supervisors.

Customer aggression prevention training further supports staff with 'Learning Bites' about preventing and managing customer aggression. 'The 4 WHYS to record' provides information to promote when and where staff record incidents of aggression and counterproductive behaviour. All customer aggression prevention Learning Bites and staff resources can be found by navigating to the relevant topic on the Customer Aggression Prevention Hub.

The Customer Aggression Training Summary outlines role required and recommended learning for; service delivery staff and their direct supervisors, staff who record, review and/or approve Managed Service Plans (MSPs).

CIMS role required learning is for all Centrelink service delivery staff and their direct supervisors. It is also role required for staff who record, review and/or approve Managed Service Plans (MSPs).

Australian Government
Services Australia

Managed Service Plan (MSP) - Customer service delivered through a One Main Contact (OMC) 104-07050060

Currently published version valid from 18/11/2025 8:15 PM

Background

s 22

s 47FE(d)

This document outlines:

- the process staff use to manage contact from customers who have a One Main Contact (OMC) arrangement as part of their Managed Service Plan (MSP)
- instructions for staff assigned as an OMC or backup OMC
- information for managers about assigning and supporting staff in these roles

MSPs with service channel restrictions are agency wide. Mutual customers across Centrelink, Medicare and Child Support must have an OMC or Personalised Services Service Officer (PSSO) assigned to help deliver services through assigned channel/s consistently.

For more information about Managed Service Plans (MSPs), see Customer aggression - Managed Service Plan (MSP).

Contact from customers who have an OMC

Once the identity of a customer or nominee/person permitted to enquire (PPE) or Update (PPU) has been confirmed, staff must observe MSP warning message and then check the customer's record for any Managed Service Plan (MSP) servicing restrictions including an assigned One Main Contact (OMC).

See the Centrelink and Medicare tab on the Process page for the steps to follow when a customer has an OMC assigned as part of their MSP.

Customers managed in Personalised Services

Contact arrangements for customers managed by a Personalised Services Service Officers (PSSO) are recorded in the Managed Service Plan (MSP). Staff must review the MSP notes to check the details of the arrangement and connect the customer with the assigned PSSO.

See Personalised Services.

Benefits of assigning an OMC

The benefits of assigning an OMC include:

- providing a consistent service offer and management of the customer's interactions
- continuity of service and a tailored approach when working with customers who are experiencing vulnerabilities, barriers or who have a history of customer aggression or counterproductive behaviour
- minimising the risk of more customer aggression or counterproductive behaviour incidents through early intervention
- educating customers about expected behaviours and obligations
- minimising the impact on service delivery of frequent and/or multi-channel customer contacts or complaints

- identifying barriers or vulnerabilities and initiating appropriate servicing strategies to provide support

A key role of the OMC is to develop, improve and, where appropriate, recover the relationship between the agency and the customer. The OMC role is critical for delivering tailored services to customers with identified vulnerabilities, barriers, complex needs or a history of aggressive or counterproductive behaviours.

OMCs build customer relationships by:

- facilitating inbound and outbound contact with the customer and establishing ongoing rapport
- accepting contact from the customer, including warm transfers from other staff within the agency (in accordance with the MSP)
- facilitating contact with other areas of the agency or external partners if needed
- ensuring procedural fairness by seeking input from customers when reviewing their MSP, see Managed Service Plan (MSP) _ Reviewing

Roles and responsibilities of the OMC

Staff assigned as a customer's OMC provide a dedicated point of contact between the customer and the Services Australia for a specified period of time (up to 12 months).

A backup OMC is assigned to cover times when the OMC is not available.

An OMC provides continuity of service and a tailored approach when working with customers who are experiencing vulnerabilities, barriers or who have a history of customer aggression or counterproductive behaviour.

When a staff member is assigned as a customer's OMC, the staff member is responsible for:

- ensuring availability to manage enquiries from the customer
- regularly reviewing the customer’s record and making proactive outbound phone contact
- resolving issues in a timely and procedurally accurate manner
- ensuring all decisions and options are clearly explained to the customer
- brokering solutions by working closely with delegates, specialist staff and external agencies to offer a holistic service experience and achieve quality outcomes for the customer
- initiating, monitoring and clearly documenting the progress, effectiveness and outcome of servicing strategies
- preparing handover information to new OMCs when leaving the role, accessing leave
- working with the customer until they are ready to be transitioned back to mainstream servicing and where possible through self-managed services

The back up OMC is required to do the OMC's role as required. They should know the customer’s MSP, including the servicing strategies and any restrictions.

Types of OMC arrangements

As part of a Managed Service Plan (MSP) an OMC may be assigned as a:

- **proactive** strategy if a customer has barriers or is experiencing vulnerability. See Identifying customer vulnerability and risk issues
- **reactive** response to an incident of customer aggression or counterproductive behaviour

The OMC arrangement is a tailored approach to customer management and can include:

- specifying contact arrangements across service channels, such as face-to-face, phone and written (including digital)
- limiting contact with the agency to prescribed times, days of the week or number of contacts
- proactively identify customer vulnerabilities, barriers and potential issues to prevent future customer aggression or counterproductive behaviour

Customers may be restricted to contacting the agency:

- at prescribed times
- on certain days of the week
- face-to-face only
- number of contacts, or
- in writing only

s 47E(d)

s 22 s 22

s 47E(d)

Assigning the OMC and backup OMC roles

Managers assign OMC and backup OMC roles based on the skills and suitability of staff to:

- communicate effectively, manage challenging customer interactions and achieve quality customer outcomes
- build rapport and establish boundaries and expectations with customers
- educate customers about their agency obligations and expected behaviours when interacting with the agency
- make procedurally fair and accurate decisions
- work with other business areas and specialists to address complex customer needs and issues

Customer Incident Management System (CIMS) processing help

MSPs for Centrelink and Medicare public customers are managed through the Customer Incident Management System (CIMS). For help with CIMS processing, see Accessing and using the Customer Incident Management System (CIMS).

The Resource page has contact details for the Customer Aggression Prevention Team (CAPT) and Complaints Team, Customer complaints and feedback index, intranet pages, Services Australia website links to Our service commitments and the Payment and Service Finder. It also has panel information links to letters and the Geographic zone map.

Related links

Customer aggression - Prevention and management

Customer aggression - Reporting and recording incidents

Customer aggression - Response

Accessing and using the Customer Incident Management System (CIMS)

Customer aggression - Staff Support

Customer aggression - Managed Service Plan (MSP)

Managed Service Plan (MSP) - Proposing, recording and approving

Managed Service Plan (MSP) - Implementing

Managed Service Plan (MSP) - Customer not complying

Managed Service Plan (MSP) - Reviewing

Managed Service Plan (MSP) - One-off variation

Personalised Services

Referring customers to and handling customer enquiries and correspondence for Personalised Services

Authenticating a Centrelink customer

Risk identification and management of threats to the safety or welfare of a child

Family and domestic violence

Identifying customer vulnerability and risk issues

Providing services to customers with disabilities

Interpreter Services for customers who are deaf or hard of hearing

Using the National Relay Service (NRS)

Recording complaints and feedback in the Customer Feedback Tool

Level 1 Manage complaints and feedback

Online Document Recording (ODR)

Payment and Service Finder

Nominee arrangements under Income Management

Reviewing nominee arrangements

Person Permitted to Enquire (PPE) or Update (PPU) authority

Sensitive Information Indicators in the CDMS

Process

This document outlines:

- the process staff use to manage contact from customers who have a One Main Contact (OMC) arrangement as part of their Managed Service Plan (MSP)
- instructions for staff assigned as an OMC or backup OMC
- information for managers about assigning and supporting staff in these roles

MSPs with service channel restrictions are agency wide. Mutual customers across Centrelink, Medicare and Child Support must have an OMC or Personalised Services Service Officer (PSSO) assigned to help deliver services through assigned channel/s consistently.

For more information about Managed Service Plans (MSPs), see Customer aggression - Managed Service Plan (MSP).

Centrelink and Medicare

This tab has the process Centrelink and Medicare staff use when a customer contacting Services Australia has an assigned One Main Contact (OMC) as part of a Managed Service Plan (MSP) in the Customer Incident Management System (CIMS).

On this page:

Customers visiting a service centre

Customers contacting a Smart Centre

MSP customer work item or contact received by a Processing Team

Customers visiting a service centre

Table 1: This table provides the steps Centrelink and Medicare staff follow when a customer visiting a service centre has an OMC arrangement as part of an MSP in CIMS.

Step	Action
1	**Authenticate the customer and confirm their OMC contact arrangements** + Read more ... • Authenticate the customer or nominee/person permitted to enquire (PPE) or update (PPU) • Unless the nominee is also a Services Australia customer with a restriction, the customer's service restriction does not apply • Identify the OMC in the MSP warning message. View the MSP in the Customer Incident Management System (CIMS). Go to Step 2 For information about locating the MSP, see **Task Card: Searching for Incident and MSP records in the Customer Incident Management System (CIMS)** on the Customer Incident Management System intranet page.
2	**Check for any service channel restrictions** + Read more ...

	Check the level of face to face service channel restriction in the MSP. An explanation of service channel restrictions is on the Resources tab on Managed Service Plan (MSP) Proposing, recording and approving. If the customer has: • a full face to face service restriction, go to Step 3 • a partial face to face service restriction, go to Step 4 • no restriction to face to face services, go to Step 5
3	**Full restriction on face-to-face services** + Read more ... s 47E(d) • **No**, see Managed Service Plan (MSP) - Customer not complying
4	**Partial restriction on face-to-face services** + Read more ... Is the customer visiting the service centre in line with the MSP arrangement? • **Yes**, ◦ Tell the OMC/backup OMC and follow their directions. If the OMC or backup OMC are unavailable, check with a team leader or manager ◦ If the OMC or backup OMC are not needed for completing the customer's business, resolve the customer's enquiry ◦ Document the contact, go to Step 6 • **No**, see Managed Service Plan (MSP) - Customer not complying
5	**No restriction on face-to-face services** + Read more ... Offer to refer the customer to the OMC/backup OMC. Does the customer want to be referred to the OMC/backup OMC? • **Yes**, ◦ Tell the OMC/backup OMC and follow their directions. If the OMC and backup OMC are unavailable, resolve the customer's enquiry ◦ Document the contact, go to Step 6 • **No**, ◦ Resolve the customer's enquiry ◦ Document the contact, go to Step 6
6	**Document customer contact** + Read more ... A note must be recorded in the MSP. Arrange for a staff member with CIMS Manager access to record the note. Email the OMC/PSSO to notify them of the customer's contact. Consider adding a note to the customer's record as per the service brand's documentation standards. For more information see: • Centrelink - Online Document Recording (ODR) • Child Support - Documenting Child Support information • Medicare - refer to the OMC/backup OMC tab to update the MSP record If an incident of customer aggression or counterproductive behaviour occurs during the interaction, record a new incident. See Customer aggression - Reporting and recording incidents.

Customers contacting a Smart Centre

Table 2: This table provides the steps Centrelink and Medicare staff follow when a customer contacting a Smart Centre has an OMC arrangement as part of an MSP in CIMS.

Step	Action
1	**Advise customer of OMC arrangements** + Read more ... Authenticate the customer or nominee/person permitted to enquire. Locate the OMC contact arrangements in the Managed Service Plan (MSP) in the Customer Incident Management System (CIMS). If an OMC/backup OMC or PSSO has been assigned, tell the customer that contact must be via the MSP arrangement. If Personalised Services (PS) managed, see Handling Centrelink customer calls at Smart Centre Call or service centre in Referring customers to and handling customer enquiries and correspondence for Personalised Services. **Note:** consult a team leader or manager for help if the customer advises they are not aware an MSP is in place. **Medicare Customers** To check if a customer has an incident recorded or MSP in place, view the customer's record in the CDMS at the Personal level. If the customer has an MSP comment in the s 47E(d) or a Sensitive Information Indicator for **Full or partial service restrictions** in the s 47E(d) , staff must see their Team Leader or Manager for help to review MSP restrictions recorded in CIMS. For help reviewing an existing MSP, see the Resources page for a link to the Health Services Delivery Division (HSDD) Customer Aggression Network Operational Contacts (CANOC). For details about locating the MSP, see **Task Card: Searching for Incident and MSP records in the Customer Incident Management System (CIMS)** on the Customer Incident Management System intranet page.
2	**Check for any service channel restrictions** + Read more ... Check the level of phone service channel restriction in the MSP. An explanation of service channel restrictions is in the Resources tab on Managed Service Plan (MSP) - Proposing, recording and approving If the customer has: • a full phone service restriction, see Managed Service Plan (MSP) - Customer not complying • a partial phone service restriction, go to Step 3 • no restriction to phone services, go to Step 4
3	**Partial restriction on phone services** + Read more ... Check the customer's servicing arrangements in the MSP or MSP letter. If the customer's restricted to contact their OMC only, see Managed Service Plan (MSP) - Customer not complying There are circumstances where a Smart Centre can resolve a customer's enquiry, these include where the customer: • can contact via phone at prescribed times and this is clearly documented in the Restrictions/Notes section of their MSP • can contact via phone at prescribed times and is permitted to speak with the Smart Centre • can contact on certain days of the week and is permitted to speak with the Smart Centre • has a restriction on the number of Smart Centre contacts they can make per day/week and have not exceeded their contact limitation. In these circumstances: • Resolve the customer's enquiry • Email the OMC and back up OMC to advise of the customer's contact

	Document the contact, go to Step 5
4	**No restriction on phone services** + Read more ... Offer to warm transfer the customer to the Personalised Services (PS) Triage line who will connect them with their OMC or backup OMC. **Does the customer want to be connected to the OMC or backup OMC?** • **Yes**, ○ Call the PS Triage line and choose option 2, and ○ document the contact, go to Step 5 • **No**, ○ resolve the customer's enquiry. Email the OMC and back up OMC to advise of the customer's contact ○ document the contact, go to Step 5
5	**Document customer contact** + Read more ... If an incident of customer aggression or counterproductive behaviour occurs during the integration, record a new incident. See Customer aggression Reporting and recording incidents. A note must be recorded in the MSP. Arrange for a staff member with **CIMS Manager** access to record the note. Email the OMC/PSSO to notify them of the customer's contact. Consider adding a note to the customer's record as per the service brand's documentation standards. For more information see: • Centrelink - Online Document Recording (ODR) • Child Support - Documenting Child Support information • Medicare - refer to the OMC/backup OMC to update the MSP record

MSP customer work item or contact received by a Processing Team

Table 3: This table provides the steps Centrelink and Medicare staff follow when a work item is allocated to a Processing team where the customer has an OMC arrangement as part of an MSP in CIMS.

Step	Action
1	**Customer has an active MSP** + Read more ... If the customer has been transferred to the Service Officer, go to Step 2 If the customer is **not** on the phone and a work item has been allocated via Workload Management, locate the OMC contact arrangements in the MSP. For details about locating the MSP, see Accessing and using the Customer Incident Management System (CIMS). **Is the customer managed by Personalised Services (PS)?** • **Yes**, see Table 2 > Step 2 in Referring customers to and handling customer enquiries and correspondence for Personalised Services. • **No**, Contact the OMC via MS teams: ○ Advise the OMC of the work item allocated for processing ○ Seek their advice on required action/s ○ Confirm if the Service Officer should contact the customer, or advise the OMC of the outcome of the work item ○ Document the record clearly based on this advice ○ Continue processing the work item based on the advice of the OMC. If the OMC is unavailable see OMC and backup OMC availability table. OMC procedure ends here.
2	**Advise customer of OMC arrangements** + Read more ...

	- Authenticate the customer or nominee/person permitted to enquire - Locate the OMC contact arrangements in the MSP - Tell the customer that contact must be via the MSP arrangement, including if an OMC/backup OMC or PSSO has been assigned - If the customer is managed by Personalised Services (PS), see Table 2 > Step 2 in Referring customers to and handling customer enquiries and correspondence for Personalised Services. Tell the customer that contact must be via the MSP arrangement, including if a PSSO has been assigned **Note:** consult a team leader or manager for help if the customer advises they are not aware of the MSP. **Medicare Customers** MSP details are recorded in CDMS as a **Sensitive Information Indicator** with the following: - Category: **Service** - Indicator Type: **Full or Partial service restrictions** - The indicator triggers a **Sensitive Information alert** when staff access the record - Staff can view the indicator details from the **Sensitive Information** pop up table or tab **Note:** consult a team leader or manager for help with the MSP servicing restrictions.
3	**Check level of service channel restriction** + Read more ... Check the level of phone service channel restriction in the MSP. An explanation of service channel restrictions is in the Resources tab on Managed Service Plan (MSP) - Proposing, recording and approving. If the customer has: - a full phone service restriction, see Managed Service Plan (MSP) - Customer not complying - a partial phone service restriction, go to Step 4 - no restriction to phone services, go to Step 5
4	**Partial restriction on phone services** + Read more ... Transfer the customer to the OMC or back up OMC: - Discuss the reason for the customer's contact with the OMC/backup OMC and the information that needs to be communicated to the customer, for example, the outcome of the claim - Warm transfer to the PS Triage line - If the customer asks for the OMC/back up and back up OMC contact details, check the MSP - If the customer wants to make a complaint, s 47E(d) s 47E(d) - If the OMC/back up OMC is not available for a warm transfer, and the customer advises that they don't have a phone number: ○ Request an alternative contact number (for example, community organisation or third party), update the customer's record and tell the customer that the OMC will contact them on this number ○ s 47E(d) ○ ○ If the customer needs social work help, consider a referral to a social worker. **Note:** it is important to contact or alert the OMC before transferring the customer to a Social Worker ○ If the customer's behaviour escalates, see Customer aggression-Response ○ Document the contact, go to Step 5 There are circumstances where a customer does not need to transfer to the OMC/back up OMC because of the partial restriction on phone servicing, these include where the customer: - can contact via phone at prescribed times and this is clearly documented in the Restrictions/Notes section of the MSP - can contact on certain days of the week and is permitted to speak with the Smart Centres - has a restriction on the number of Smart Centre contacts they can make per day/week and have not exceeded their limit

	In these circumstances: - Resolve the customer's enquiry - Email the OMC and back up OMC to advise of the customer’s contact - Document the contact, go to Step 6
5	**No restriction on phone services** + Read more ... Offer to warm transfer the customer to the OMC/backup OMC. **Does the customer want to transfer to the OMC or backup OMC?** - **Yes**, ○ call the PS Triage line ○ warm transfer the call ○ document the contact, go to Step 6 - **No**, ○ resolve the customer's enquiry. Email the OMC and back up OMC to advise of the customer’s contact ○ document the contact, go to Step 6
6	**Document customer contact** + Read more ... If an incident of customer aggression or counterproductive behaviour occurs during the interaction, record a new incident. See Customer aggression Reporting and reporting incidents. A note must be recorded in the MSP. Arrange for a staff member with CIMS Manager access to record the note. Email the OMC/PSSO to notify them of the customer's contact. Consider adding a note to the customer's record as per the service brand's documentation standards. For more information see: - Centrelink - Online Document Recording (ODR) - Child Support - Documenting Child Support information - Medicare - refer to the OMC/backup OMC to update the MSP record

OMC/backup OMC

This tab has instructions for staff assigned as the One Main Contact (OMC) and backup OMC as part of a customer's Managed Service Plan (MSP) in the Customer Incident Management System (CIMS). The OMC may be a Personalised Services Officer (PSSO).

Note: the OMC/Backup OMC must be granted s47E(d) so that they can search for, access, and update a customer’s MSP. Refer to Accessing and using the Customer Incident Management System (CIMS)

On this Page:

OMC and backup OMC availability

Table 1

Category title	Description
Availability of OMC and backup OMC	**OMC and backup OMC availability** + Read more ...

	As a customer's single point of contact the OMC must be available for contact from the customer and to accept call transfers from other staff in the agency. To makes sure this happens: • OMC should update their contact details in ESS • The OMC must promptly return customer calls within 3 business hours, when they have received a call back email from Personalised Services • The backup OMC must be familiar with the contact arrangements and servicing strategies for the customer. The OMC can do this by discussing the arrangement with the backup OMC and maintaining accurate notes in the MSP **Note:** if the OMC and/or back up OMC will be unavailable for a period of time, they should discuss this with the **Employee Responsible** of the MSP. Depending on the length of the absence, the **Employee Responsible** may either appoint a new OMC/backup OMC or make other temporary OMC servicing arrangements. For more information, see Table 1 on the Employee Responsible tab. Document all contact attempts and outcomes in the MSP, see Document contact.

Commencement of MSP

Table 2: This table describes the initial customer contact requirements for staff assigned as the OMC and backup OMC as part of a customer's MSP.

Task	**Action required**
Preparation for contact	**Check the customer's record** + Read more ... Check: • the details of the MSP including its duration and any servicing arrangements • if the customer has received the MSP letter • the triggering incident (if reactive MSP), including the agency business that the customer was conducting when incident occurred • previous incidents (leading up to the triggering incident) • vulnerabilities or complex issues (e.g. homelessness, mental health, incarceration; language barriers, contact details) • outstanding business (e.g. unfinalised or rejected claims; debts; payment related issues) • other business areas involved in the customer's record, such as an Authorised Review Officer, the Participation team, Debt recovery • servicing strategies, including internal and external referrals • if the customer is a mutual Child Support and/or Medicare. The OMC will coordinate business across programs. Cross program OMCs should liaise with subject matter experts if they are unfamiliar with legislation, policy or processes Contact with the MSP customer provides: • the opportunity to explore underlying triggers • the customer with the opportunity to explain what happened and why
OMC across service delivery brands	**Service delivery brands** + Read more ... The MSP will have 2 mandatory Servicing Strategies: • Review and update MSP details in CUBA • Review and update MSP details in CDMS These mandatory strategies are implemented as restrictions may be applied across all service brands i.e. Centrelink, Medicare and Child Support. When the MSP was created in CIMS, the strategies may have been actioned and display as **Completed** or **Not Required**. If the status of these strategies remains as **Not Started**, the OMC will need to action these.

Initial contact	**Contact customer immediately when assigned** + Read more ... A letter is sent to the customer upon approval of the Managed Service Plan (MSP). For information about MSP letter delivery methods see Managed Service Plan (MSP) Proposing, recording and approving and Managed Service Plan (MSP) Implementing. In some serious cases, police may hand the letter to the customer. If this occurs, it must be recorded in the MSP. The MSP letter should still be delivered according to the relevant method. Attendance at a service centre in non compliance with the servicing restriction may be an offence under the relevant trespass laws and actions may be taken should attendance occur. s 47E(d) s 47E(d) Attempt to contact the customer before they get the MSP implementation letter. This provides an opportunity for the OMC to introduce themselves and proactively establish expectations for future interactions. Topics for discussion may include (but is not limited to): • An explanation of the role of the OMC and the reasons why an OMC has been assigned • Information about the period of the OMC arrangement • The objectives of the agency for assigning an OMC • When and how the customer can contact the OMC • Right to ask for a review of the MSP • For a face to face restriction, advice about what to do if they need to attend (for example, for an appointment, or get a letter with a request that is inconsistent with their restriction), see Face to face contact with customers • Contact details for the OMC/backup OMC. Provide the PS Triage line phone number, with option 1 or 2 depending on whether the customer is managed by Personalised Services or by a local OMC. Consider issuing an OMC Contact Card. See Resources page for a link on how to order the OMC/PSSO contact cards • Contact arrangements if the OMC is unavailable (also notify the backup OMC) • An outline of the expected behaviours for both the OMC and customer, to encourage a mutually respectful relationship from the start of the arrangement. The Resources page includes a link to the agency's service commitments on the Services Australia website • Discuss enquiries the customer has raised and address any unresolved issues • Ask the customer if they are a mutual customer of Centrelink, Medicare and/or Child Support as liaison with other programs may be needed Document details of discussion. In the MSP record a s 47E(d) note. In the note include the following details: • Contact reason: (Commencement of MSP) • Time: • Discussion: • Behaviour and warnings: • Updates to record: Complete the s 47E(d) field on the s 47E(d) page of the MSP.
OMC/PSSO Contact card	**One Main Contact (OMC)/Personalised Services Service officer (PSSO) contact cards** + Read more ... To order cards, submit a request via the s 47E(d) portal. Alternatively, order cards from the s 47E(d) intranet page. The card template must have the following fields: • **Name:** (insert PS Triage line phone number) • **Position:** 8:30am to 4:30pm • **Division/Branch:** Contact: • Leave other fields blank Select s 47E(d) . Preview the business card to ensure it displays correctly.

	The card can be issued to the customer by: - attaching to the following letters: ○ MSP implementation ○ MSP reminder ○ MSP review outcome - issuing when the customer has advised that they have lost their OMC/PSSO's details - issuing when the customer breaches their MSP, if safe to do so
Document contact	**Document all contact and contact attempts** + Read more ... Document all customer contact in the MSP notes, including voicemail messages left by the customer that relate to the MSP and details of unsuccessful contact attempts. Document contact not related to the MSP on the customer's system record, for example a decision about social security payments. See Online Document Recording (ODR).

Ongoing customer management

Table 3: This table describes ongoing customer management expectations for staff assigned as the OMC and backup OMC as part of a customer's MSP.

Task	Action required
Regular health checks	**Health checks** + Read more ... Conduct regular 'health checks' (recommended fortnightly) to pre-empt issues that may lead to the customer contacting outside of their MSP restrictions. Regular contact provides an opportunity to identify changes in the customer's circumstances and build rapport. The 'health-check' should include checking for: - upcoming/outstanding issues (reporting, participation issues, overpayments, unactioned work) - the progress of any claims, enquiries, appeals or complaints - payment related issues (debts, arrears, deductions, garnishees) - letters recently sent or received - further incidents recorded - upcoming appointments - changes in circumstances The regular health check also provides an opportunity to progress the MSP's Servicing Strategies.
Customer incarcerated	**Health checks for incarcerated customer** + Read more ... Health checks for customers with a **confirmed** incarceration period of longer than 6 months can occur less frequently. The recommended health check regularity for incarceration periods is: - 4 weekly for 6 -12 months - 12 weekly for 12-24 months - 26 weekly for over 24 months To confirm the incarceration period, email the Incarcerated Customer Program team: s 47E(d) - - - - **Note:** health checks are not limited to the recommended regularity. More frequent checks can be done if necessary due to customer circumstances. Examples include customers with a:

	• nominee • pending claim • debt activity where action is required
Regular contact	**Regular contact with customers** + Read more ... After conducting a health check of the customer's record, consider if an outbound call is required to discuss any outstanding business. If there is no outstanding business, a proactive call will give the customer an opportunity to advise any new information. Topics for discussion may include: • progress of any current activities • reporting (if required) • online services • progress of servicing strategies Document details of discussion: • Record a note in the MSP using relevant note type: o s47E(d) , or o s47E(d) , or o s47E(d) The note should include the following details: • Contact reason: • Time: • Discussion: • Behaviour and warnings: • Updates to record: • Progress/Outcome of servicing strategies: • Referrals: • Follow up actions: Document all unsuccessful contact attempts, including if a decision is made to not contact the customer, using the note type: s47E(d) .
Document all contact and contact attempts	**Document all contact and contact attempts** + Read more ... Document all customer contact in the MSP notes, including voicemail messages left by the customer that relate to the MSP and details of unsuccessful contact attempts. Document progression and outcomes of Servicing Strategies. Document contact not related to the MSP on the customer's system record, for example a decision about social security payments. See Online Document Recording (ODR).
Customer not complying with OMC arrangements	**Non-compliance with OMC arrangements** + Read more ... If the customer is not complying with the OMC arrangements in the MSP, see Managed Service Plan (MSP) - Customer not complying.
New incidents of customer aggression and counterproductive behaviour	**Reporting incidents of customer aggression and counterproductive behaviour** + Read more ... Record any subsequent incidents of customer aggression or counterproductive behaviour that occur during the MSP period. See Customer aggression - Recording and reporting incidents.
Complaints	**Managing customer complaints** + Read more ... Record all complaints lodged by the customer (including complaints related to the OMC arrangement), see Recording complaints and feedback in the Customer Feedback Tool. Manage the customer feedback, see Level 1 - Managing complaints and feedback. If the customer lodges online feedback, assess the feedback and decide who is best placed to manage it. If possible, the OMC should manage all open complaints for the customer. If the OMC can

	manage the online feedback, assign the OMC as the employee responsible in the s47E(d) of the Customer Feedback Tool and follow feedback management procedures, see Level 1 Online customer feedback. Seek guidance, advice or support on complaint management from the Escalated Complaints Team.
Return to sender – MSP letters	**Returned to sender - Managed Service Plan (MSP) letters** + Read more ... Returned MSP letters do not result in an automatic suspension with a reason of 'Whereabouts Unknown' (WUK) nor the creation of an associated Work Item to alert staff of the returned item. For information about the Return to Sender process, see Managed Service Plan (MSP) – Implementing.
Nominee arrangements	**Appointing and reviewing nominee arrangements** + Read more ... Nominees can act on behalf of customers in certain circumstances and assist customers to engage with us. While there are no automatic reviews for nominee arrangements, OMCs/PSSOs should take the opportunity to review voluntary arrangements during the MSP period. For example: • when requested by the customer/nominee • risk factors that may impact on their ability to act in the customer's best interests • where family and domestic violence are a concern in the customer's relationship with the nominee/proposed For more information see: • Adding or rejecting a nominee request • Reviewing nominee arrangements
Communication from other agency staff	**Providing advice on customer behaviour and service** + Read more ... OMCs may be contacted by other staff, including Authorised Review Officers (ARO), Random Review Teams, Complex Assessment Officers (CAO), Participation teams when conducting business for the customer. OMCs should monitor the customer's behaviour and assess their circumstances to provide advice to the Customer Aggression Operational Contact (CANOC) Employee Responsible, .Decision makers and specialist panels. Contribute to the development of service strategies for the customer. This may involve being asked to give information to panels, the Employee Responsible and other specialists
New OMC assigned	**Handing over to new OMC** + Read more ... The new OMC must contact the customer in accordance with the instructions for Initial contact with the customer in the Customer contact by OMC/Back up OMC table. **See also:** Table 1 on the Employee Responsible tab.
Servicing strategies	**Servicing strategies updates** + Read more ... OMCs are required to: • progress servicing strategies in the customer's MSP • document the progress and outcome of each servicing strategy Servicing Strategies are flexible and can be changed to meet the changing circumstances of the customer. The OMC may recommend that a servicing strategy is added or removed.
One-off variation	**One-off MSP variation** + Read more ... s 47E(d)

	s 47E(d) See Managed Service Plan (MSP) One off variation.
MSP review input by OMC/Backup OMC	**MSP review** + Read more ... The OMC plays an important role when reviewing the MSP, including assessing ongoing risk. See Managed Service Plan (MSP) - Reviewing.
Guidance, advice and support	**Seeking expert advice and support** + Read more ... The OMC may seek guidance, advice and support in relation to MSPs and customer aggression from the: • Customer Aggression Network Operational Contact (CANOC) • Customer Aggression Prevention Team (CAPT) The Resources page includes a link to these intranet pages.

Transfer of an MSP customer to a new Service Zone (Centrelink and Medicare (HSDD) customers only)

Note: a zone transfer of a current MSP customer occurs when there is a permanent change to their residential address to a different zone.

Table 4

Step	Action
1	**Customer has changed zone** + Read more ... OMC/PSSO become aware that a customer's geographic zone has changed. Contact the customer to confirm if their address change is permanent, unless it is not appropriate, based on the limited circumstances of the case. If permanent, refer the case to the Zone Customer Aggression Network Operational Contact (CANOC) for action. Not all long-term change of zones will result in a transfer. In some situations, a transfer would not be best for Services Australia and the customer. These include: • incarceration / involuntary institutionalisation • homelessness, risk of homelessness or unstable accommodation • ongoing transience • if a customer is experiencing vulnerability and risk issues and is effectively managed in the current zone and a transfer may result in more aggression • if an MSP is at a critical point in resolving trigger(s) of aggression In these situations, if it is unclear that a transfer should occur, zone CANOCs should consult and determine where the customer is best managed. Is the change of zone permanent or has the risk of moving been assessed by both zones? • **Yes**, go to Step 2 • **No**, continue current management of the customer. Procedure ends here
2	**Customer has moved permanently to another zone and will be transferred** + Read more ... The current OMC/PSSO will include a handover note in the MSP and advise their CANOC: The note includes: • progress of Servicing Strategies

	• details of further incidents and MSP compliance • any unresolved triggers of aggressive behaviour • frequency and reason for contacts • contact preferences • current commitments/actions
3	**Send email to receiving zone CANOC** + Read more ... The sending zone CANOC must email the receiving zone CANOC with the: • MSP ID • end date of current MSP (flag email as urgent if within 28 days) • new address • request to identify a new OMC, backup OMC and contact details **Note:** the receiving zone will respond to the sending zone within 5 business days, with the new OMC details. Is the MSP due to end within 28 days? • **Yes**, go to Step 4 • **No**, the existing OMC should tell the customer of the details of their new OMC. Go to Step 5
4	**When the MSP ends within 28 days** + Read more ... The sending zone completes the MSP review - see, Managed Service Plan (MSP) - Reviewing. If an MSP is to be extended, the sending zone completes and approves the MSP and advises the receiving zone via email. If a Provisional MSP is expiring, the receiving zone will be invited to attend the panel meeting.
5	**Updating MSP and send letter/SMS to customer** + Read more ... The receiving zone reviews the MSP and updates: **General Details** • The new Service Zone • New One Main Contact (OMC) and backup OMC • New Employee Responsible **Strategies and Referrals** • Add any new servicing strategies Remove any servicing strategies, which are no longer applicable.
6	**New OMC** + Read more ... The receiving zone CANOC/OMC/PSSO issues an MSP letter notifying of the change in OMC and attaches the letter to the MSP. The new OMC/PSSO contacts the customer to introduce themselves and advise: • their MSP is continuing in their new location • how they can contact the OMC • ongoing self service options • any changes to their servicing strategies as a result of the relocation Manage the customer as per Customer service delivered through a One Main Contact (OMC) as part of a Managed Service Plan (MSP). PSSO - Refer to Personalised Services.
7	**Ongoing management of customer** + Read more ... The receiving zone CANOC must include the customer on the agenda of their next panel meeting to make sure local leadership/specialists are aware of the transfer.

Employee Responsible

s 47E(d)

This tab describes the factors the s 47E(d)) must consider when assigning, reassigning and supporting the One Main Contact (OMC) and backup OMC as part of a customer's Managed Service Plan (MSP).

Assigning, changing and supporting the One Main Contact (OMC) and backup OMC

This table describes the factors to be considered by a manager when assigning, reassigning and supporting the OMC and backup OMC as part of a customer's MSP.

Task	Action required
Consider OMC arrangements	**Selecting appropriate OMCs** + Read more ... After an incident of customer aggression or counterproductive behaviour consider the service channel or method of contact that balances the needs of the customer with any safety risk posed to staff, other customers and Services Australia. s 47E(d) Types of OMC contact arrangements are most often reflected through service channel restriction details in the MSP. Some examples include but are not limited to the following. **Face-to-face channel:** • Full face-to-face restriction: Customers with a full face-to-face servicing restriction are prohibited from entering Services Australia premises. An OMC must be assigned to provide the customer with contact details by phone or in writing • Partial face-to-face restriction. Customer contact is restricted to: ○ a pre-arranged appointment with the OMC (customer must contact OMC to arrange the appointment) ○ a prescribed day or time, or ○ a specific number of times per day **Phone channel:** • Phone contact with OMC (no limitation to day or time of contact) • Phone contact with OMC partially restricted to a prescribed day/time or number of times the customer can contact agency per day **Written channel:** • An OMC must be assigned when a customer has been advised they can only contact the agency in writing, including digital services **Consider customer circumstances** Check if the customer has a valid working phone number and current address. If a customer is not contactable by phone or does not have a fixed address then alternative arrangements should also be considered. Advised the customer that every Telstra payphone in Australia is free to use. s 47E(d)

	For more information about identifying customer vulnerability and risk issues, see Identifying customer vulnerability and risk issues. s 47E(d) **Note:** if it is identified that the customer is at risk, or experiencing homelessness or unstable accommodation that has not previously been recorded, see Homelessness Indicators. **OMC across service delivery brands** Depending on the customer's current circumstances and level of interaction with all programs, consider who the most suitable OMC will be options include an OMC for each program or an OMC who will coordinate business with each program on behalf of the customer. Cross program OMCs should liaise with program subject matter experts if they are unfamiliar with legislation, policy or processes.
Assigning OMC staff	**Assigning OMC and backup OMC roles** + Read more ... Staff assigned as OMC and backup OMC should be suitably skilled and trained to deliver services to customers with identified vulnerabilities, barriers or a history of aggressive or counterproductive behaviour. If staff have been impacted by an incident, it is not appropriate to assign them as the OMC/backup OMC for the customer involved in the incident. Examples of staff suitably skilled to undertake the OMC role include, but are not limited to: • Subject Matter Experts (APS4 staff and higher) • Social Workers • Indigenous Service Officers • Team Leaders • Managers
CIMS Access level	**CIMS access level requirements** + Read more ... The OMC/Backup OMC must hold CIMS Manager access so that they can search for, access, and update a customer's MSP. Refer to Accessing and using the Customer Incident Management System (CIMS).
Changing OMC arrangements	**Changing the OMC** + Read more ... The OMC role may be reassigned to a different staff member when: • the customer makes a reasonable request for review of their MSP and/or OMC and there are reasonable grounds for assigning a new OMC • the customer changes location and it is appropriate to assign a new OMC • the agency determines the customer's circumstances are better managed by a different OMC • the OMC will be temporarily unavailable. i.e. fewer than 30 days. The Employee Responsible adds s47E(d) to the MSP stating: s47E(d) • the OMC is unavailable for more than 30 days. E.g. changes role or leaves the agency The Employee Responsible must review OMC arrangements and consider appointing new OMCs when: • the OMC will be unavailable for more than 30 days, or • both the OMC and backup OMC will be unavailable at the same time **Note:** if a new OMC is appointed, the customer must be advised of the new OMC (in writing and by phone).
Supporting OMC staff	**Supporting OMC staff** + Read more ... Managers need to:

	- Support the OMC to conduct regular health checks of customer records - Make sure the backup OMC can support the OMC in the event of leave or unavailability. Consider workload reallocation if the OMC and backup OMC will both be unavailable - Support the OMC to work through any barriers or challenges with the customer - Review any complaints made by customers about the OMC arrangement. This may result in a review of the MSP - Access call recordings if appropriate. See Call and screen recording information and access - Make sure OMC staff are aware of the support available to them, see Customer aggression Staff Support

References

Legislation

s 22

Freedom of Information Act 1982

Public Order (Protection of Persons and Property) Act 1971 (POPPPA)

Resources

Contact details

Customer Aggression Prevention Team (CAPT)

Complaints

Personalised Services

Incarcerated Customer Program team > F2F Incarcerated customer contacts

Note: the **Leadership Positional Mailbox** for incarcerated customer servicing **must** be used.

Customer Incident Management System (CIMS) intranet page

Customer Incident Management System

Complaints and feedback index

Complaints and feedback index

Intranet links

Customer Aggression Prevention Hub

Corporate Support Business Card Request

Ordering business cards, employee contact cards, name badges and desk plates

Managing incidents of customer aggression and MSP's

For Customer Aggression Network Operational Contacts, see **Networks** tab on Customer Aggression Prevention Hub

Multicultural and Tailored Services Branch

Local Assessment Panels (LAPs) and Zone Assessment Panels (ZAPs) Structures

Services Australia website

Service commitments

Payment and Service Finder

Accessibility

MSP letter templates

The letters available via this link are endorsed for use by Services Australia and are the latest versions. Staff should not be using locally produced letters.

General Correspondence see Customer aggression

Geographic zone

Services Australia Boundaries and Office Locations

Training & Support

A summary of CIMS Role Required Learning with relevant LMS codes and a range of additional training and reference material is available on the Customer Aggression Prevention Hub.