



Inland Revenue
Te Tari Taake



**MINISTRY OF SOCIAL
DEVELOPMENT**
TE MANATŪ WHAKAHIATO ORA

Memorandum of Understanding

**between Inland Revenue (IR) and
the Ministry of Social Development (MSD)**

for

COVID Income Relief Payments

**Pursuant to the Approved Information Sharing Agreement under Part
9A of the Privacy Act 1993 and Part 3, section 18E of the Tax
Administration Act 1994**

June 2020

Released Under The Official Information Act 1982

This Agreement is made effective on the date of the last signature and is

Between Inland Revenue (IR)
And Ministry of Social Development (MSD)

(the Parties)

1. Interpretation

1.1. The following terms used in this MOU have the following meanings unless the context requires otherwise:

Term	Meaning
AISA	The Approved Information Sharing Agreement authorised by the Privacy (Information Sharing Agreement between Inland Revenue and Ministry of Social Development) Order 2017 http://legislation.govt.nz/regulation/public/2017/0176/latest/DLM7358754.html?src=qs .
Applicant	A person that applies for CIRP, whether entitled to it or not.
Business Owner	An employee of each Party as designated in this MOU who will oversee the on-going operation of this MOU.
Certificate of Confidentiality	A certificate of confidentiality as required by section 18B(2) of the TAA in the form prescribed by the Commissioner of IR from time-to-time.
CIRP	COVID Income Relief Payment.
COVID-19	The novel coronavirus, see: https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus .
Expiry Date	31 August 2021, or any extended date as agreed by the parties in writing.
Income	Salary and wage income including Accident Compensation payments, paid parental leave and schedular income payments.
Information	Information that may be shared by IR and MSD under this MOU, as specified in the Schedules.
IRD Number	A unique identifier assigned by IR.
MOU	This Memorandum of Understanding between IR and MSD as amended from time to time, including any Schedules.

MSD Portal	The portal that IR has developed to give MSD Portal Users direct access to Information in START for the purposes of this MOU.
MSD Portal Users	Any MSD employee with the delegated authority to access information held in START for the purposes of this MoU.
Partner	A person who is the partner of an Applicant.
Party	IR or MSD (as the context requires), and Parties means both IR and MSD.
Personnel	Any employee, agent, contractor or representative of a party.
Recipient	An Applicant or a Partner who has received CIRP, whether entitled to or not.
SFTP	Secure file transfer protocol.
START	IR's Simplified Tax and Revenue Technology System.
TAA	Tax Administration Act 1994.

1.2. In this MOU, unless the context requires otherwise, references to:

- a. clauses and Schedules are to clauses and Schedules to this MOU;
- b. the singular includes the plural and vice versa; and
- c. any statute includes any amendment to, or replacement of, that statute and any subordinate legislation made under it.

2. Background

2.1. On 12 March 2020, the World Health Organisation announced that the COVID-19 (a new strain of coronavirus) outbreak qualified as a pandemic.

2.2. In response to the pandemic, containment measures were put in place in New Zealand. These measures have had a significant economic impact on businesses and individuals that has required a Government response.

2.3. For individuals who have lost their employment as a result of COVID-19, the Government announced a new non-taxable welfare payment - the COVID Income Relief Payment (CIRP). This payment is authorised under section 101 of the Social Security Act 2018.

2.4. From 8 June 2020, CIRP is available for up to 12 weeks to eligible people who have ceased employment because of the impact of COVID-19 from 1 March to

30 October 2020 inclusively. The last payment date of CIRP will be 22 January 2021, and the CIRP programme will expire on 20 February 2021.

- 2.5. To maintain the integrity of the CIRP programme, MSD and IR will share Information with each other via SFTP and the MSD Portal for the purposes specified in clause 4.

3. Legal Authority

3.1. IR will disclose Information to MSD, and MSD will disclose Information to IR, under this MoU in accordance with the AISA.

3.2. The AISA authorises sharing for the purpose of:

- a. assessing eligibility for, and entitlement to, benefits and subsidies; and
- b. assessing and enforcing any obligations relating to benefits and subsidies, including recovering any associated debt.

CIRP is a monetary payment that falls within the definition of benefits in the Social Security Act 2018 and in the AISA.

3.3. Regardless of the legal authority for sharing the Information, IR and MSD will only share Information to the extent that is necessary to achieve one or more of the purposes in clause 4.

4. Purpose and Use

4.1. IR may supply Information to MSD to enable MSD to administer CIRP, including to:

- a. assess whether an Applicant is entitled to CIRP;
- b. verify any relevant information that MSD holds about the Applicant or their Partner (if relevant);
- c. review and audit CIRP payments to determine whether Applicants or their Partners received any amount of CIRP they were not entitled to receive;
- d. investigate whether Recipients received any amount of CIRP they were not entitled to receive; and
- e. take proceedings to recover any amount of CIRP that a Recipient was not entitled to receive.

4.2. MSD may provide Information to IR so that IR can:

- a. compare it against information that it holds to assist MSD in determining which Applicants are eligible to receive CIRP;
- b. assist with MSD's review, audit, investigative and prosecution processes in relation to Recipients and payments;

- c. run risk profiling business processes which use income information to query entitlements; and;
- d. understand an IR customer's income sources to enable discussions about their entitlements and capability to repay debt.

5. Governance process

5.1. The Business Owners will be responsible for the operation of this MOU.

5.2. The functions of the Business Owners include:

- a. co-ordinating the supply and delivery of Information;
 - b. discussing and coordinating Information quality issues;
 - c. agreeing in principle to modify any aspect of this MOU;
 - d. identifying policy and systems changes at an operational level;
-
- e. co-ordinating joint MSD and IR reviews of security and procedures for this MOU where either Party consider that a review is necessary, or in any event at least once before the Expiry Date;
 - f. establishing and maintaining good relations between the Parties;
 - g. resolving any issues or disputes between the Parties that are referred to the Business Owner from either Party; and
 - h. reporting to their Chief Executive and Commissioner in relation to this MOU, as required.

5.3. At the date of this MOU, the Business Owners are as follows:

IR	MSD
<p>Section 9(2)(a) [Redacted]</p> <p>Network Lead Customer Experience Asteron Centre 55 Featherston St PO Box 2198 Wellington</p> <p>DDI: Section 9(2)(a) [Redacted]</p> <p>Section 9(2)(a) [Redacted] @ird.govt.nz</p>	<p>Warren Hudson General Manager, Integrity and Debt Client Service Support National Office Level 8, The Aurora Centre 56 – 66 The Terrace Wellington</p> <p>DDI: Section 9(2)(a) [Redacted]</p> <p>Section 9(2)(a) [Redacted] @msd.govt.nz</p>

5.4. A Party may change its Business Owner, or their contact details, by giving the other Party's Business Owner written notice of the change via email.

6. Security

- 6.1. Each Party will communicate Information to the other Party using the secure transmission methods specified in the Schedules .
- 6.2. Each Party will each keep the Information it receives from the other Party in a secure environment and safeguard it from unauthorised access.

7. Accuracy of information

- 7.1. The Parties acknowledge that the Information is the most up-to-date Information that a Party holds at the time it is provided, but neither Party makes any representation as to the accuracy of the Information.
- 7.2. Before using any Information obtained under this MOU, the Parties agree to take reasonable steps to ensure that the Information is complete, accurate, relevant, up-to-date and not misleading.
- 7.3. Reasonable steps may include:
- a. confirming the information is not already held by MSD;
 - b. confirming the Information with the individual concerned; and
 - c. confirming the Information with the source of the information (e.g. employer).
- 7.4. The Parties note that:
- a. The Privacy Commissioner has approved a reduced adverse action notice period (decreased from 10 days to 5 days) under the AISA in respect to MSD taking adverse action against Applicants that MSD identify as not eligible, or no longer eligible, for CIRP.
 - b. The Privacy Commissioner approval is subject to the conditions set out in Schedule 5.

8. Reporting

- 8.1. The Parties will monitor the communication of Information under this MOU and may report within their respective organisations on the:
- a. volume of Information communicated;
 - b. nature of Information communicated;

- c. protections applied to the use of Information;
- d. errors or problems with the Information; and
- e. complaints received.

8.2. The Parties note that Information sharing under this MOU is subject to reporting requirements issued by the Privacy Commissioner under the AISA. MSD will provide any necessary reporting to IR so that IR can comply with those reporting requirements.

9. Privacy and Confidentiality

9.1. The Parties must comply with their obligations under the Privacy Act 1993, the Official Information Act 1982, the TAA and the Social Security Act 2018.

9.2. MSD must keep confidential any Information it receives and may only use or disclose the Information to the extent necessary for the purposes of this MOU.

9.3. Before an MSD staff member or anyone engaged by MSD receives or has access to any Information that IR provides, he or she must execute a Certificate of Confidentiality. MSD must retain all signed Certificates of Confidentiality and make them available to IR on request.

9.4. If a Party receives a complaint or request under the Privacy Act 1993 or the Official Information Act 1982 relating to the sharing of Information under this MOU, it will consult with the other Party before responding.

10. Breaches of privacy, confidentiality, or security

10.1. All breaches of this MOU must immediately be notified to the Business Owners and any actual or suspected unauthorised disclosures of the Information must be investigated.

10.2. Where an investigation is undertaken, IR and MSD will provide each other with reasonable assistance through the Business Owners and keep each other informed of progress.

10.3. If either IR or MSD has reasonable cause to believe that any breach of privacy, confidentiality, or any security provisions in this MOU has occurred or may occur, IR and MSD may undertake such investigations in relation to that actual or suspected breach as either deems necessary. IR and MSD shall ensure that they provide each other with all reasonable assistance in connection with such inspections or investigations.

- 10.4. If there has been a breach of privacy, confidentiality, or any security provisions in this MOU, either IR or MSD may suspend this MOU to give each other time to remedy the breach. While the MOU is suspended, neither Party may communicate Information to the other Party.

11. Responsibility for acts and omissions of Personnel

- 11.1. The Parties will be responsible for the acts and omissions of their respective Personnel. In particular, each Party will:
- a. keep its Personnel informed of their privacy, security and confidentiality obligations relating to the Information, including the requirements of the TAA, the Privacy Act 1993, Official Information 1982 and this MOU;
 - b. ensure its Personnel are adequately trained to perform the agreed tasks;
 - c. ensure that its Personnel are contractually bound to comply with their privacy, security and confidentiality obligations relating to the Information; and
 - d. ensure access to the Information is not available to any of its Personnel who is not covered by or who has not complied with all of the above requirements of this clause.

12. Variations to this MOU

- 12.1. If a Party proposes a variation to this MOU, it must give reasonable notice of the proposed variation, and the reason for the proposed variation, to the other Party.
- 12.2. Any variation to the main body of this MOU must be in writing and signed by the signatories to this MOU, or their delegates.
- 12.3. Variations to, or additions of, Schedules to this MOU must be agreed in writing by the Business Owners by exchange of email.

13. Dispute resolution

- 13.1. If an issue or a dispute ("dispute") arises in relation to this MOU, the Business Owners will meet in good faith to attempt to resolve it as quickly as possible.
- 13.2. If the Business Owners are unable to resolve the dispute within 60 days, the dispute may be referred in writing to IR's Commissioner and MSD's Chief Executive, or their delegates.
- 13.3. The Parties will continue to comply with their obligations under this MOU despite the existence of any dispute.

14. Term, termination and expiry

- 14.1. This MOU commences on the date it is last signed (and may be signed in counterparts). It continues in effect until terminated in writing by either Party, or until the Expiry Date (whichever is the earlier).
- 14.2. The requirements of this MOU concerning privacy, security and confidentiality shall remain in force notwithstanding the termination or expiry of this MOU.

15. Record-keeping


- 15.1. Information collected under this MOU that becomes part of an MSD or IR record (such as records relating to Recipients) will be retained to the extent required by the Public Records Act 2005.

16. Costs

- 16.1. Each Party will cover their respective costs associated with the arrangements described in this MOU.

SIGNATORIES


Signed for and on behalf of **Inland Revenue** by:



Date: 01 / 07 / 2020

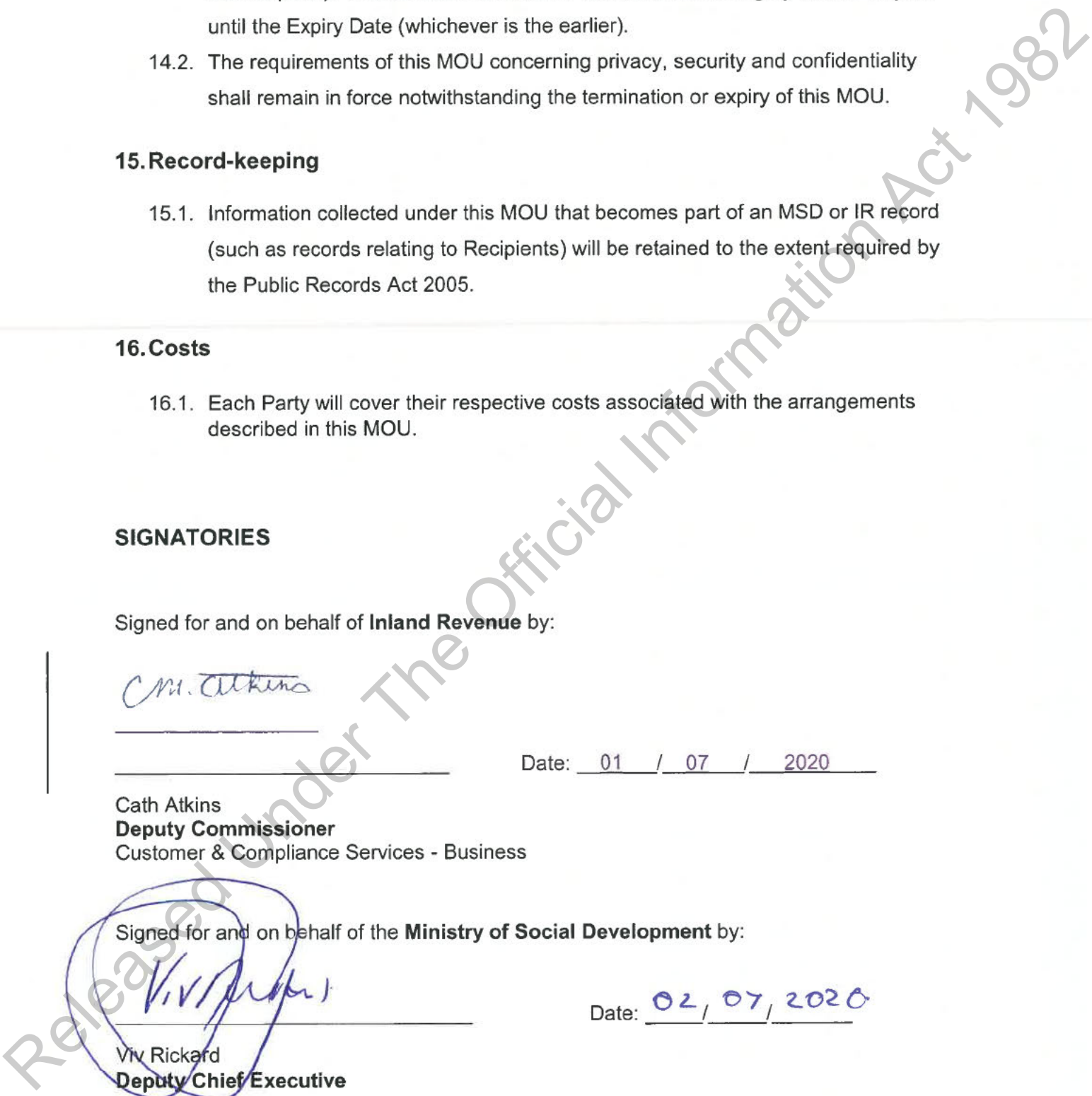
Cath Atkins
Deputy Commissioner
Customer & Compliance Services - Business

Signed for and on behalf of the **Ministry of Social Development** by:



Date: 02 / 07 / 2020

Viv Rickard
Deputy Chief Executive



Schedule 1

Information Sharing Overview

The Parties may share Information as specified in the following Schedules:

- a. Schedule 2: Information MSD and IR share weekly via SFTP to assist MSD to administer CIRP.
- b. Schedule 3: Information MSD shares with IR monthly via SFTP to assist IR with assessing entitlements.
- c. Schedule 4: Information IR shares with MSD via the MSD Portal to assist MSD to administer CIRP.
- d. Schedule 5: Adverse Action Conditions

Released Under The Official Information Act 1982

Schedule 2

Information MSD and IR share weekly via SFTP to assist MSD to administer CIRP

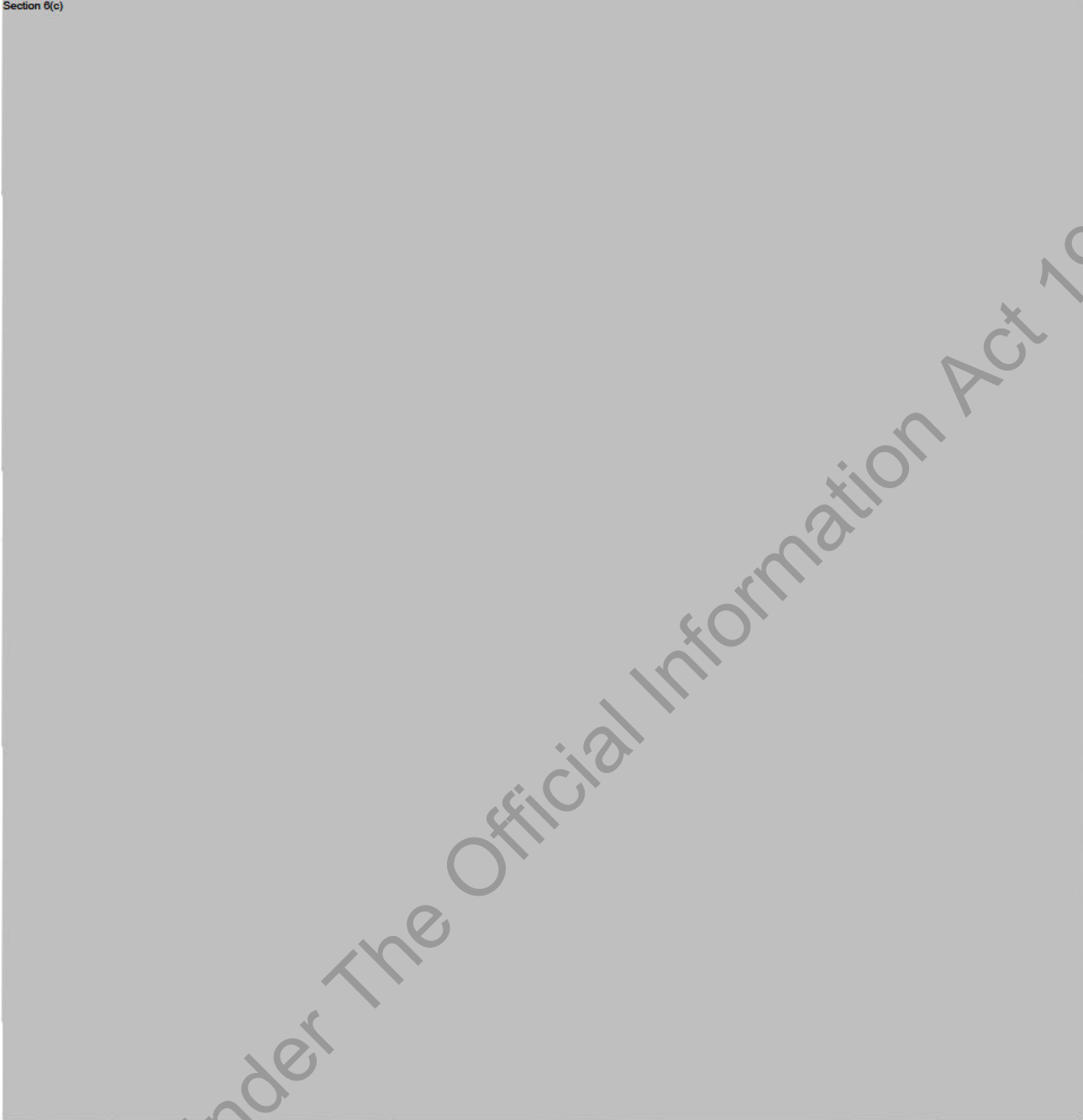
Operational Details

Key Details		
1.	Expected benefits as a result of the sharing	<ul style="list-style-type: none"> • Provide temporary income relief payments to people who are unemployed as a result of Covid19 • Identification of Income discrepancies between information held by IR and MSD • Information to enable enforcement action to be undertaken to recover payments • New intelligence about systemic abuse of the CIRP programme
2.	Expected adverse actions	<ul style="list-style-type: none"> • Suspension of a Recipient's CIRP • Creation of CIRP overpayments on client records • Investigation and prosecution of CIRP fraud • CIRP recovery actions

Operational Process		
3.	Outline of end to end operational process	<ul style="list-style-type: none"> • MSD will send a list containing the Information set out in row 10 of this table to IR via SFTP for a random selection of Recipients • IR match Recipient data with their data base and provide a response via SFTP • Where the data does match to an IR customer, IR will send the Information set out in row 13 of this table for that Recipient to MSD via SFTP • MSD will retain the list for 60 working days for reporting purposes, recording the number of Recipients sent to IR and the number matched • Where there is an Income match, this data will be collated into a separate report which will be loaded into MSD's work flow management tool, Straight to Processing (S2P) • Users allocated to the CIRP Audit queue will be pushed a task showing the information from MSD and IR, side by side • The user will ensure that the Recipient's details match. (If it is not a match, the case will be closed and IR notified that it was not a match). • If it is an Income match, the user will check MSD systems to ensure the Income information is not already held

Operational Process		
		<ul style="list-style-type: none"> • If the Income information is not held in MSD systems, the user will phone the Recipient to let them know MSD has matched their information with IR which shows they are or have been receiving Income from an employer • If the user is not successful in contacting the Recipient by phone, a text and email will be sent asking the Recipient to contact MSD • If no contact is made within 2 days, a notification in the form of a letter will be sent to the Recipient, advising them of the match information and asking that they contact MSD within 5 days to discuss. The client will receive an email or text alerting them that there is a new letter which can be viewed in MyMSD (which all CIRP applicants had to sign up to when applying). If we can see that a client has opted out of viewing their letters via MyMSD, the (pdf) letter will be emailed to the client. The letter will also be posted to the client. If the Recipient does not contact MSD, their CIRP may be stopped. • If the Recipient makes contact, the user will check with the Recipient regarding the Income and take the appropriate action regarding CIRP, e.g. no action required as the Income was from their previous employer, or payments will stop and a debt may be established. • If the Recipient doesn't contact MSD within 5 days of receiving the letter, the user will use data from the MSD Portal to determine entitlement to CIRP • If the CIRP is stopped and a debt created, the Recipient will be advised of this and given the right of review
4.	MSD record selection	<ul style="list-style-type: none"> • Current recipient of CIRP • Start date no less than four weeks prior to selection for review
5.	Number of records per supply	To be determined following testing
6.	Frequency of supply	Weekly
7.	Transmission mechanism / protocol used	SFTP
8.	MSD transfer job name	CIRP Random Audit
9.	IR transfer job name	MSD CIRP Validation

Section 6(c)



Released Under The Official Information Act 1982

Section 8(c)



Released Under The Official Information Act 1982

15.	MSD system/database(s)	<ul style="list-style-type: none">• Retained in Information Analysis Platform (IAP)• Processed in S2P, CMS and SWIFTT
-----	------------------------	--

Information Exchanges		
	where data is processed / retained	
16.	MSD retention period	<ul style="list-style-type: none"> 60 working days or longer period if required for enforcement purposes.

Reporting		
17.	Details of audit activities including scope and frequency	<ul style="list-style-type: none"> IR MSD AISA every two years
18.	Agency responsible for audit activities	<ul style="list-style-type: none"> Inland Revenue is lead agency for the AISA and sections 96S and 96U of the Privacy Act specify IR may be required to report on certain aspects of operations of the AISA.

Released Under The Official Information Act 1982

Schedule 3

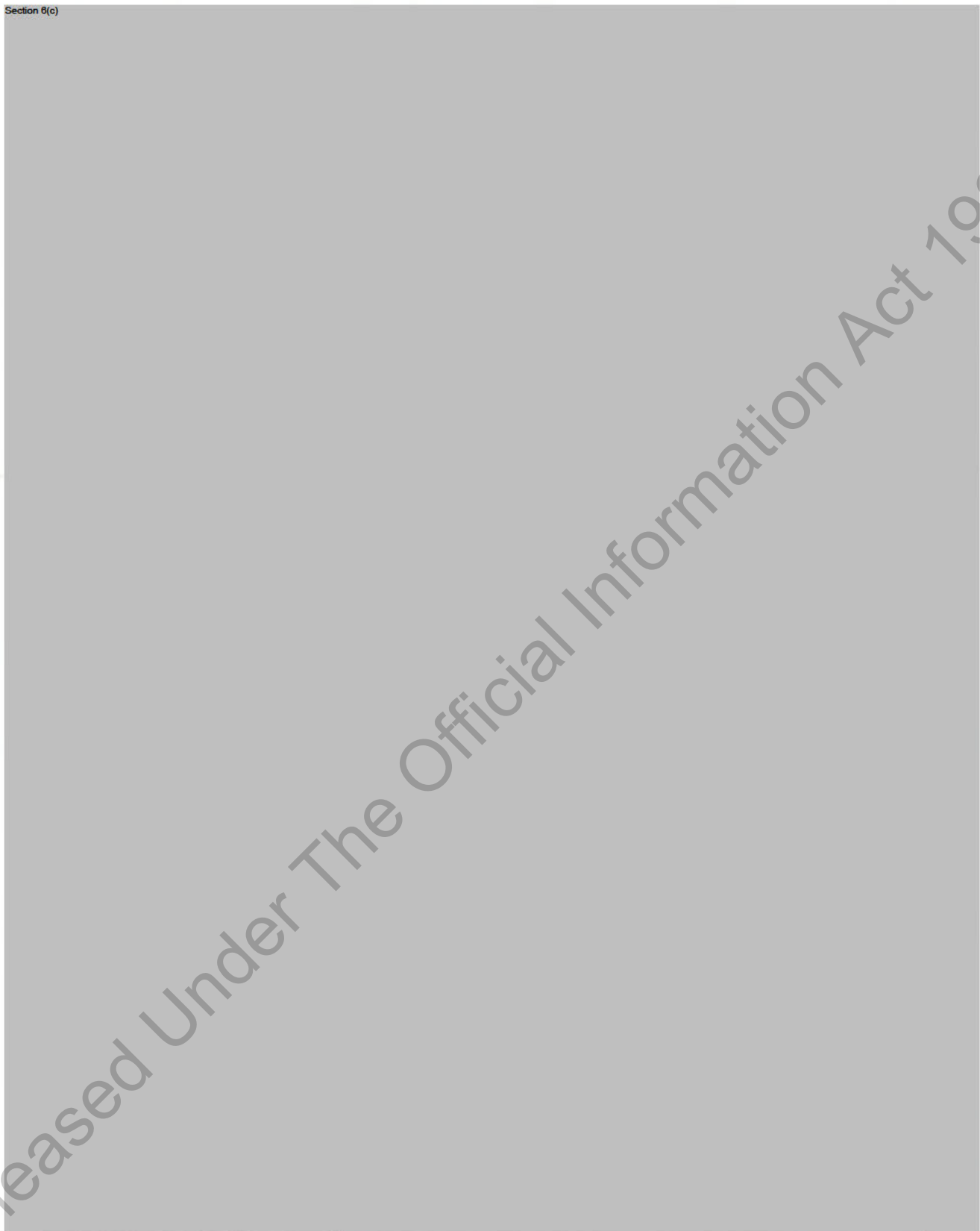
Information MSD shares with IR monthly via SFTP to assist IR with assessing entitlements

Operational Details

Key Details	
Expected benefits as a result of the sharing	<ul style="list-style-type: none"> • Reduce unnecessary contacts with IR customers through IR's automated discovery processes • Full visibility about an IR customer's income sources to accurately determine entitlements and capability to repay debt
Expected adverse actions	IR does not anticipate taking any adverse actions

Operational Process	
Outline of end to end operational process	<ul style="list-style-type: none"> • MSD will send a monthly file of Recipients to IR via secure SFTP • IR will load the data into the data warehouse within START • The data will be incorporated into START processes to ensure appropriate system actions are taken and customer accounts will be flagged in START to enable IR front line staff to communicate effectively with these customers
MSD record selection	Any Recipient that has been approved payment of CIRP
Number of records per supply	Number will be based on the number of new applications approved in the previous calendar month
Frequency of supply	Monthly at the end of each month until CIRP complete
Transmission mechanism / protocol used	SFTP
MSD transfer job name	Recipients approved in previous month
IR transfer job name	MSD CIRP recipients

Section 6(c)



Released Under The Official Information Act 1982

IR retention period	Retained to the extent required by the Public Records Act 2005
---------------------	--

Reporting	
Details of audit activities including scope and frequency	<ul style="list-style-type: none">IR MSD AISA every two years
Team responsible for audit activities	<ul style="list-style-type: none">Inland Revenue is lead agency for the AISA Audit and sections 96S and 96U of the Privacy Act specify IR may be required to report on certain aspects of operations of the AISA

Released Under The Official Information Act 1982

Schedule 4

Information IR shares with MSD via the MSD Portal to assist MSD to administer CIRP

Information disclosure

1. IR may share the Information specified below with MSD via the MSD Portal to support MSD's CIRP audit, review, investigation and prosecution processes between 08 June 2020 and the Expiry Date.
2. Search terms to be used by MSD:
 - a. Search for a Recipient by IRD Number, or name and date of birth.
 - b. When searching by name and date of birth, the surname name and date of birth are required.
 - c. Only current active Recipients with an unrestricted security type are visible in the search results.
 - d. IRD Number in the search results provides a hyperlink to a screen displaying more detail about the Recipient as set out in clause 3 of this Schedule
3. Information that IR may make available in response to search terms:
 - a. First name and surname.
 - b. IRD Number.
 - c. Date of Birth.
 - d. Recipient's address.
 - e. A list of active employer relationships with employment payment dates.
 - f. An Income breakdown that displays Income that a Recipient has received within a specified date range.
 - g. Income only available from 90 days before 1 March 2020.
4. IR may disclose the Information to MSD Portal Users via the MSD Portal. The privacy of Recipients whose personal information may be accessed through the MSD Portal will be protected by the following types of controls:
 - a. **User Access Controls:** controls that will allow only appropriate MSD Portal Users to access the MSD Portal; and
 - b. **User Process Controls:** controls that manage what the users can see and do with Information accessed through the MSD Portal.

5. Access to the MSD Portal for the purposes set out in this MOU will be limited to MSD Portal Users. Access will be available 24/7 except for midnight Sundays to 4am Mondays.
6. The role of MSD Portal Users is to use the MSD Portal to check information held by MSD, to determine whether it matches the Information available in response to the search terms, via the MSD Portal.
7. Each MSD Portal User will be assigned to a Manager within MSD. The role of the Manager is to:
 - a. add and remove MSD Portal Users;
 - b. use the MSD Portal's audit capabilities to ensure that MSD Portal Users are only using the MSD Portal for the purposes of this MOU; and
 - c. create monthly reports to provide information to IR about how the MSD Portal has been used by MSD Portal Users.

User Access Controls

8. As required under clause 9.3 of the main body of the MOU, each MSD Portal User must sign a Certificate of Confidentiality. As at the date of the MOU, the form includes the following provision, which signatories acknowledge when signing the form:

"I understand that knowingly not completing this certificate before acquiring, obtaining, or having access to the information described above, or knowingly not complying with the requirements to keep such information confidential, is an offence under sections 143D to 143EB of the Tax Administration Act 1994."
9. MSD must maintain a list of the MSD Portal Users who have signed a Certificate of Confidentiality. Managers must not add user access for any person without firstly sighting a signed Certificate of Confidentiality.
10. Each MSD Portal User will use their MSD email address as part of the user set up process. It will not be possible to set up a user account for MSD Portal Users with any other type of email address (e.g. a personal or non-MSD business email address).
11. The set-up process will require a second factor of authentication. This will be in the form of a one-time use code that will be sent by IR to the MSD Portal User. The code will be sent to the MSD email address supplied for the MSD Portal User.
12. Each MSD Portal User will be assigned a unique username and password. A password cannot be used by anyone other than the MSD Portal User to whom it was originally assigned. MSD Portal Users will be automatically blocked from access to the MSD Portal if they make 6 incorrect password attempts.
13. MSD Portal Managers can take the following actions to manage MSD Portal User access:

- a. Set up new MSD Portal User accounts.
 - b. Remove an MSD Portal User's account, thereby removing their access to the MSD Portal.
 - c. Reset an MSD Portal User's password, thereby either:
 - i. Blocking the MSD Portal User's access to the MSD Portal until their new password is activated via the MSD Portal User's MSD email address; or
 - ii. unlocking an MSD Portal User's access if they have been locked out due to incorrect password attempts.
 - d. Reinstate access to the MSD Portal for any MSD Portal User whose access to the MSD Portal has been blocked.
 - e. Enable access to the individual search functionality for a maximum of 50 MSD Portal Users for CIRP purposes.
 - f. Undertake monthly reviews of MSD Portal users and ensure removal of inactive MSD Portal Users.
14. MSD Portal Managers must ensure that MSD Portal Users will only be assigned to work on CIRP related audits, reviews, investigations and prosecutions.
15. MSD Portal Managers will not be able to carry out searches of the Information listed in clauses 2 and 3 of this Schedule.
16. MSD Portal Users who have not accessed the MSD Portal for 60 days will be automatically blocked from access to the MSD Portal.
17. MSD will provide IR with a whitelist of approved IP addresses. It will not be possible for an MSD Portal User to access the MSD Portal from any device whose IP address is not on that whitelist. The whitelist will be restricted to MSD approved devices and will not include personal devices.
18. The MSD Portal will be configured so that it can only be accessed using whitelisted devices via an approved MSD network. That will include MSD's corporate network, and VPN, but will exclude public and personal wi-fi networks.
19. Any attempt to access the MSD Portal through any means not approved in this Schedule may amount to a breach of the MSD Code of Conduct and constitute grounds for disciplinary action.
20. IR reserves the right to revoke any MSP Portal User's access to the MSD Portal at any time.

User Process Controls

21. MSD Portal Users will have read-only access to the Information listed at clause 3 of this Schedule, and no other IR data, via the MSD Portal. That data is the information that is necessary to assist MSD to undertake its audit, review, investigation and prosecution processes for CIRP.
22. All use of the MSD Portal by MSD Portal Users will be monitored by an MSD Portal Manager. The Manager will be able to see details of all actions taken by the MSD Portal User whilst using the MSD Portal. That includes, but is not limited to:
 - a. every keystroke and mouse click in the MSD Portal;
 - b. every search undertaken;
 - c. every click-through on every search result; and
 - d. the amount of time spent in each MSD Portal screen.
23. MSD Portal Managers and IR will regularly monitor MSD Portal Users' use of the MSD Portal to ensure that it is being used in accordance with the terms of this MOU.
24. Any misuse of the MSD Portal by any MSD Portal User identified by MSD or IR will be drawn to the attention of the other Party as soon as practicable, and access to the MSD Portal by that MSD Portal User will be suspended until further investigation has taken place.
25. MSD Portal Users will be governed by the MSD Code of Conduct and will be expected to follow the Code of Conduct rules when accessing and using IR Information. Failure to comply with the Code of Conduct may amount to grounds for disciplinary action.
26. MSD Portal Users and MSD Portal Managers will receive training before they use the MSD Portal. The training materials will be developed jointly by MSD and IR. Training will enable MSD Portal Users and Managers to:
 - a. Access the MSD Portal, and understand the Information available through the Portal, to enable MSD to undertake its audit, review, investigation and prosecution processes for CIRP.
 - b. Access the minimum amount of Information through the MSD Portal necessary to assist MSD to undertake its audit and review processes for CIRP
 - c. Respect the privacy rights of any individuals whose personal information is available to them in the process of using the MSD Portal.

- d. Understand the controls detailed in this Schedule, and the implications of not complying with them, including the possible consequences of breaching the confidentiality requirements set out in the Certificate of Confidentiality.
- e. Understand the procedures to follow if the MSD Portal is unavailable for use for any reason.
- f. Understand the procedures to follow to report a suspected breach of security, confidentiality or privacy, or to raise any user queries about use of the MSD Portal.

27. Respecting the privacy rights of Recipients includes but is not limited to:

- a. Only using the MSD Portal to access information that is necessary to undertake audit, review, investigation and prosecution processes for CIRP. That includes but is not limited to a prohibition on accessing the IR records of any friend, relative, colleague, or associate, even if any such person makes a request for their records to be accessed.
- b. Not using the functionality of any device to extract, download, copy, record, capture, snip or disseminate Information that is available through the MSD Portal other than in accordance with clause 36 of this Schedule.

IR shall:

- 28. Be responsible for the security of the MSD Portal's information and infrastructure.
- 29. Work with MSD to develop appropriate training for MSD Portal Users and MSD Portal Managers.
- 30. Ensure an audit trail is available that will show which IR data has been accessed by which MSD Portal Users.
- 31. Report any security, confidentiality or privacy breaches to MSD as soon as reasonably possible after any such breach is identified. The point of contact at MSD for reporting breaches will be detailed in the training materials.

MSD shall:

- 32. Maintain a register of all MSD Portal Users that are authorised to access the MSD Portal.
- 33. Collate the signed Certificates of Confidentiality and, as required under clause 9.3 of the main body of the MOU, make them available to IR on request.
- 34. Ensure that MSD Portal Users and MSD Portal Managers receive appropriate training, covering the points summarised at clauses 26 and 27 of this Schedule.
- 35. Cooperate with IR to ensure that appropriate **Access** and **Process** controls, as outlined in this Schedule, are in place to manage access by MSD Portal Users to the MSD Portal.

36. Not extract, download, copy, record, capture, snip or disseminate IR customer's personal information that is available through the MSD Portal for transfer to MSD systems, but may use Information reviewed on the MSD Portal to manually update details in MSD systems to the extent permitted under this MoU. The only information that MSD Portal Users will extract from the MSD Portal will be limited to reports run by Managers on MSD Portal User activity, for the purposes of ensuring compliance with these controls.
 37. Ensure that MSD Portal Users' access to the MSD Portal is terminated within 5 working days after they no longer require access.
 38. Conduct regular dip samples of MSD Portal Users' activity in the MSD Portal, to ensure that the MSD Portal is only being used in accordance with the terms of this MOU.
 39. Provide a report to IR no less infrequently than every month, detailing the MSD Portal Users' activity in the MSD Portal. The purpose of that report is to provide assurance that the MSD Portal has only been used in accordance with the terms of this MOU.
-
40. Report any security, confidentiality or privacy breaches to IR as soon as reasonably possible after they have been identified. The point of contact at IR for reporting breaches will be detailed in the training materials.

Released Under The Official Information Act 1982

Schedule 5

Adverse Action Conditions

The Privacy Commissioner's approval of a reduced adverse action notice period (decreased from 10 days to 5 days) under the AISA in respect to MSD taking adverse action against Applicants that MSD identify as not eligible, or no longer eligible, for CIRP is subject to the following conditions:

1. MSD is required to ensure that all Applicants have the adverse action process adequately explained in advance, noting the shortened notice period.
2. MSD is required to provide follow up notice when adverse action is taken.
3. MSD is required to take all reasonable steps to make contact with an Applicant to notify them of:
 - a. the discrepancy;
 - b. the proposed adverse action; and
 - c. the information that would be needed in order to avoid the adverse action.
4. MSD is required to monitor for 'undelivered email' notifications and, where such notifications are received, MSD must take steps to remedy the failed communication or deliver a notice of adverse action using an alternative method.

Released Under The Official Information Act 1982