Minimum Metadata Capture Standard

Approved by:	Privacy and Security Oversight Board (PSOB) on 03/05/2021
Next Review	03/05/2023
Standard Owner:	General Manager Information

1 Standard

1.1 Scope

1.1.1 This standard applies to MSD information assets covered by relevant Disposal Authorities (DA) and "Archives New Zealand's General Disposal Authority (GDA) - 6 Common corporate service public records", but not "General Disposal Authority (GDA) 7 Facilitative, transitory, and/or short-term value records".

1.2 Minimum Metadata Requirements

1.2.1 Metadata comes in multiple forms – free-text, controlled lists and automatically generated.

1.2.2 Metadata **must** be captured for all information assets stored in MSD approved repositories, so they can be appropriately managed throughout the information lifecycle.

1.2.3 Metadata forms part of the information asset so **must** be attached throughout the information lifecycle.

1.2.4 Metadata **must** be a design component of all approved repositories of Ministry information.

1.2.5 The Information Group **must** advise System Owners on what level metadata **must** be applied (e.g. to individual records, or whole datasets).

1.2.6 To manage information assets through their lifecycle, the following **must** be required.

- Creator (e.g. individual and/or entity)
- Creation/Collection date
- Classification (in line with the classifications in scope of MSD Information Classification Standard)
- Unique identifier e.g. Object ID
- Name / Title
- Type / Format (unstructured data only)
- Audit trails minimum (read only):
  - User
  - Date of access
  - Action taken
- Modification date
- Modifier (e.g. individual or automated)
- Modification (e.g. information classification change)
- External sharing (where applicable) e.g.
  - What was shared
  - What agency it was shared with (not individual)
  - When it was shared (includes when it is/was received)
- Retention and Disposal Class
- Disposal trigger date (where applicable, Information Group to advise)
- Date of Disposal
- Disposal Action (e.g. Delete or Transfer)

- Evidence of disposal e.g. stub (where applicable, Information Group to advise)

The Information Group will advise how, when and where these are applied.

1.2.7　The System Owner *must* ensure this standard is upheld to information in their repository.

1.2.8　The System Owner *must* ensure read-only metadata cannot be altered.

1.2.9　The metadata schema *must* be documented outside of the system so that metadata fields are used in the way they were intended and aligned to the schema.

1.2.10　The Information Asset Owner *must* approve any metadata settings and setting changes with advice from the System Owner and the Information Group. The System Owner is responsible for implementing the agreed settings.

2　Standard Compliance

2.1　Exceptions

2.1.1　If any requirements from this standard cannot be met, the Information Asset Owner and/or the Systems Owner *must* contact the Information Group to seek an exception.

2.1.2　Exceptions *must* be applied for using the approved exceptions process.

2.2　Compliance Measurement

2.2.1　Compliance to this standard will be measured through various methods, including but not limited to monitoring, business tool reporting, internal and external audits, reviewing system configuration documentation and consultation with information asset owners and system owners.

3　References

Information Governance Policy

Information Classification Standard

Retention and Disposal Standard

Archives New Zealand Metadata for information and records

Archives New Zealand General disposal authorities

4　Definitions

Word/phrase	Definition
Approved repository	A repository approved by MSD that meets business, legislative and information requirements.
Dataset	A collection of structured data. Can also contain embedded unstructured data.
Disposal Action	Processes associated with implementing information destruction or transfer which are documented within disposal authorities and can only be applied by the Information Group.

	Transfer refers to the transfer of control of information to Archives New Zealand, or an authorised party.
Disposal Authority (DA) & General Disposal Authority (GDA)	An information management instrument that defines the disposal actions that are authorised for specified records and can only be applied by the Information Group. • General Disposal Authorities • GDA6 Common corporate service public records • GDA7 Facilitative, transitory, and/or short-term value records • MSD's current Disposal Authority (DA694)
Individual record	Information that we create or receive that relates to the business functions and activities of MSD. It is generally kept as evidence of business activities and transactions, or to meet legal, audit and business requirements.
Information	Recorded data or information in any form or medium, created or received and maintained as evidence of Ministry business (including processes, advice, activities, and decision-making). This includes, but is not limited to, documents, signatures, text, images, sound, speech or data and can come in a variety of formats such as electronic and paper files, email correspondence, film, tape, computer discs, text messages, social media, and web pages.
Information Asset	An Information Asset is an identifiable collection of data or information recognised as having value to the agency. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Asset Owner	Information Asset Owners (IAOs) are senior individuals responsible for understanding what information is held, what is added and what is removed, how information is moved, and who has access and why. IAOs are responsible for ensuring that the asset's value to MSD is fully realised and that it is used appropriately. The IAO role includes providing assurance and making sure that action is taken where required.
Metadata	Metadata is descriptive information e.g. the name, creator, creation date etc. It helps people to find, understand, authenticate, trust, use and manage information assets. Can be user or system generated.
Metadata schema	Logical plan showing the relationships between metadata elements, normally through establishing rules for the use and management of metadata.
Record set	A collection of individual records.
System Owner	A Systems Owner is responsible for the overall operational and maintenance of a system where information is held, including any

	related support service, and ensuring all governance processes are followed and business requirements are met.

Information Retention and Disposal Standard

Approved by:	Privacy and Security Oversight Board (PSOB) on 03/05/2021
Next Review	03/05/2023
Standard Owner:	General Manager Information

1   Standard

1.1   Scope

1.1.1   This standard applies to all MSD information created and collected for Ministry business that is subject to the Public Records Act 2005.

1.2   General

1.2.1   Information retention and disposal is a fundamental activity in an information asset's lifecycle and the Information Group *must* ensure that it is regular and systematic.

1.2.2   All Ministry information *must* be stored in the appropriate line of business system so that information retention and disposal can be applied.

1.2.3   The System Owner *must* ensure that an information asset is accurate, up to date, and available for the life of the asset.

1.2.4   The System Owner *must* ensure that the information asset is in a useable, complete, and appropriate format; and protected against unauthorised modification and corruption.

1.2.5   If a System Owner discovers that an information asset has been corrupted, they *must* immediately contact the Information Group to determine the disposal action as appropriate.

1.2.6   *Only* the Manager Information Management has the authority to assign ownership to the General Manager Information.

1.2.7   Information retention and disposal schedules as described in relevant Disposal Authorities (DA) and General Disposal Authorities (GDA) *must* be adhered to.

1.3   Appraisal

1.3.1   Information assets eligible for disposal *must* first be appraised, and this activity *must* be undertaken by the Information Group.

1.3.2   Appraisal *must* be documented in consultation with the Information Asset Owner and System Owner.

1.3.3   The Information Asset Owner *must* agree to the retention and disposal settings for their information assets including frequency of disposal, triggers and other system reporting as required by the Information Group's advice.

1.3.4   The Information Group *must* approve all information retention and disposal settings.

1.4 Implementation

1.4.1 Any disposal actions *must* be approved by the relevant Information Asset Owner before implementation.

1.4.2 Any disposal action *must* be authorised by the Manager Information Management before implementation to ensure that relevant parties have been engaged, and that the appropriate Disposal Authority has been identified and documented.

1.4.3 The System Owner is responsible for ensuring that when an information asset is disposed it is permanently destroyed and cannot be recovered for ongoing use by the business.

1.4.4 The Information Group *must* notify the Information Asset Owner once the disposal actions have been completed, and the Information Group *must* update the Information Asset Register once disposal has been actioned.

1.4.5 Once the disposal action has been completed on an information asset, a metadata record *must* be retained. If a metadata record cannot be retained within the line of business system, the system owner *must* contact the Information Group for advice.

2 Standard Compliance

2.1 Exceptions

2.1.1 If any requirements from this standard cannot be met, the Information Asset Owner and/or the System Owner *must* contact the Information Group to seek an exception.

2.1.2 Exceptions *must* be applied for using the approved exceptions process.

2.2 Compliance Measurement

2.2.1 Compliance to this standard will be measured through various methods, including but not limited to monitoring, business tool reporting, internal and external audits, system documentation review and consultation with Information Asset Owners and System Owners.

3 References

Public Records Act 2005

Archives New Zealand General Disposal Authorities

Ministry of Social Development Disposal Authority

Information Governance Policy

Minimum Metadata Standard

Protective Security Requirements

Information Classification Standard

4   Definitions

Word/ phrase	Definition
Appraisal	The process of evaluating business activities. Includes analysis of business context, business activities and risk to enable decision making on what records to create and capture, and how to ensure the appropriate management of information over time.
Destruction	Process of eliminating or deleting information beyond any possible reconstruction.
Disposal Action	Processes associated with implementing information destruction or transfer which are documented within disposal authorities and can only be applied by the Information Group. Transfer refers to the transfer of control of information to Archives New Zealand, or an authorised party.
Disposal Authority (DA) & General Disposal Authority (GDA)	An information management instrument that defines the disposal actions that are authorised for specified records and can only be applied by the Information Group. • General Disposal Authorities • GDA6 Common corporate service public records • GDA7 Facilitative, transitory, and/or short-term value records • MSD's current Disposal Authority (DA694)
Information	Recorded data or information in any form or medium, created or received and maintained as evidence of Ministry business (including processes, advice, activities, and decision-making). This includes, but is not limited to, documents, signatures, text, images, sound, speech or data and can come in a variety of formats such as electronic and paper files, email correspondence, film, tape, computer discs, text messages, social media, and web pages.
Information Asset	An information asset is an identifiable collection of data or information recognised as having value to the agency. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Asset Owner	Information Asset Owners (IAOs) are senior individuals responsible for understanding what information is held, what is added and what is removed, how information is moved, and who has access and why. IAOs are responsible for ensuring that the asset's value to MSD is fully realised and that it is used appropriately. The IAO role includes providing assurance and making sure that action is taken where required.
Metadata	Metadata is descriptive information e.g. the name, creator, creation date etc. It helps people to find, understand, authenticate, trust, use and manage information assets. Can be user or system generated.

System Owner	A System Owner is responsible for the overall operational and maintenance of a system containing information, including any related support service, and ensuring all governance processes are followed and business requirements are met.

Steps to Freedom (StF)

This page will give you information and supporting materials to help you with the Steps to Freedom process.

On this Page:

What is Steps to Freedom

Steps to Freedom (StF) is a special needs grant paid to people who were in prison or held in custody on remand for 31 days or longer; and have been released from prison or from court. StF are also paid to deportees (deported from overseas (back to New Zealand) following release from prison) – Please refer to Map. StF special need grant is to help with essential costs to re-establish themselves back in the community.

StF payments are normally made onto a Westpac card for ease of use but can be made by direct credit to a client or agents account.

How Steps to Freedom payments are issued

Scheduled releases from prison

Department of Corrections work with MSD staff members (usually a Prisoner Reintegration Coordinator (PRC)) to advise us of upcoming scheduled releases. This will allow PRCs (or other staff members) to determine entitlement and arrange a StF payment loaded onto a Westpac card, for their release day.

Unscheduled release from court

A person who is released from court will most likely walk into an MSD Service Centre to apply for their StF payment.

The Service Centre will confirm that they are eligible for a StF payment. Staff will check how best to make the payment (i.e., direct credit to a bank account). If direct credit is not an option, the Service Centre will hold a supply of Westpac StF cards.

Unscheduled releases from prison

Each prison has a supply of **pre-loaded** Westpac debit cards locked in an on-site safe. These cards are retained for unscheduled releases. **Note:** this may include court hearings via audio/visual links.

Department of Corrections staff will provide a pre-loaded Westpac debit card, green MSD payment card (if available), and the MSD handout for the use of the StF card for unscheduled releases if the person is eligible (i.e. has been in custody for 31 or more days).

Corrections will keep a register of Westpac debit cards provided and provide these registers to MSD within 1 business day so that we can reconcile the StF payments onto client records.

Activating Westpac cards

StF payments are made through CMS Hardship. Westpac cards need to be activated, by submitting a task via S2P to Crown Revenue to approve. Full instructions here.

Key information about the Westpac Steps to Freedom cards

The card is only for a Steps to Freedom payment – it is not an ongoing bank account and can not be re-loaded

- To use the card:
  - At any ATM machine: select **CHEQUE** and use the pin number on the back
  - Eftpos or online purchases: select **CREDIT** and use the Pin number on the back
- Westpac cannot provide any support at branches, or over the phone.
  Do not refer clients to Westpac. If they require a balance, this can be done at an ATM
- The client handout has more information and should be issued with every card

Download the client handout (PDF 270.7KB)

Error messages and declined transactions

- Error messages usually mean the wrong account has been selected, or wrong pin used
- Check the client is using the correct one – cheque at ATM machines, but credit at EFTPOS machines
- If wrong details are repeatedly used, the card will lock
  - This lock will lift the next day.

- If a card declines, clients should confirm the available balance via an ATM
- If they require hardship assistance until the card unlocks, assess as per business standards

Pending transactions

- This is where the card shows one amount for the 'balance' but a different amount for funds 'available'
- There are several reasons this may occur:
- Type 1: Delay. A client may have paid for a product, e.g. bread from the dairy, but the dairy doesn't process its banking until the next day, so the card balance still shows as $350 even though the client bought bread.
- Type 2: Hold. Like a bond, some retailers might hold a payment on a client's card. For most of our clients, they'll get the money back within two days. For example:
  - Paying at the petrol pump - please advise clients not to do this as the machine "holds" $150, no matter the amount of petrol they buy. The remainder won't come back to the card for about 24hrs – to avoid this they should go into the petrol station and pay directly.
  - Hotels often hold the full amount for a stay eg. two nights, even if they only stay for one. The unused payment won't be refunded for at least 24hrs.

Please note: If you escalate card queries to the Crown Revenue team, they can't see what type of "pending transaction" it is in the banking portal. While most retailers sort their banking within two days, we have no way to guarantee when this will happen.

If it is necessary to investigate further please escalate to **all three** email addresses with the full Westpac StF card number (16 digits, on the front of the card), and the client's SWN:

- s9(2)(a) OIA
- s9(2)(a) OIA
- Crown Revenue s9(2)(a) OIA

Ordering Westpac Steps to Freedom cards

If a Service Centre requires more cards

All sites can order StF cards in S2P.

- Navigate to S2P, 'Add Processing', search for "Crown Revenue"
- Select, "New Cheque Book/Steps to Freedom Cards Request"
- On the next page:
  - Select "Westpac Steps to Freedom card".
  - In the comment field, write how many Steps to Freedom cards your site needs. We recommend:
    - Sites with low StF volumes, estimate StF card order based on expected volumes for 3-6 months.
    - Sites with higher STF volumes (e.g. close to prisons or courthouses), please order cards monthly.

Crown Revenue will ensure a steady supply of cards from Westpac.

If a Corrections facility requires more cards

The delegated contact at each Corrections facility will email MSD Crown Revenue at crown_revenue@msd.govt.nz to ensure one point of contact between agencies.

The number of cards held at each Corrections facility will vary. Prison sites are responsible for ensuring the number of cards ordered is sufficient to cover an MSD site being closed for at least a week.

The card order email must include:

- the number of cards required, will vary from site to site
- the prison name and location for cards to be sent to
- contact details for two Corrections' staff at this prison delegated to order cards.

Please do not contact Crown Revenue on behalf of the prisons.