

State Records Authority of New South Wales

General Retention and Disposal Authority - Source records that have been migrated (GA33)

This general retention and disposal authority is approved under section 21(2)c of the *State Records Act 1998* following prior approval by the Board of the State Records Authority of New South Wales in accordance with section 21(3) of the Act.

General Retention and Disposal Authority – Source records that have been migrated (GA33) © State of New South Wales through the State Records Authority, 2008. This work may be freely reproduced and distributed for most purposes, however some restrictions apply. See the copyright notice on www.records.nsw.gov.au or contact State Records.

ISBN 978-0-9805148-4-1

State Records Authority of New South Wales General Retention and Disposal Authority

Authority no GA33

SR file no 08/0223

Scope

The purpose of this general retention and disposal authority is to provide for the authorised disposal of State records which have been used as the input or source records for successful migration operations.

Public office

This general retention and disposal authority applies to all NSW public offices.

Approval date

2/09/2008

Alan Ventress
Director
State Records Authority of New South Wales

Date

Table of contents

1	Overview	6
1.1	Purpose of the authority	6
1.2	What records does the authority cover?	6
1.3	Conditions for the destruction of records	6
1.4	Records excluded from this authority	7
1.5	Status of this authority	7
1.6	How long is this authority in force?	7
1.7	For more information.....	7
2	Records authorised for disposal	8
3	Guidelines for use.....	9
3.1	About migration.....	9
3.2	Conditions for the destruction of records	10
3.3	Records excluded from this authority	16
3.4	Relationship to other General Retention and Disposal Authorities	18
3.5	Destroying digital records	18
	Appendix 1: Requirements from State Records <i>Standard on Digital Recordkeeping</i>	19

1 Overview

1.1 Purpose of the authority

The purpose of this general retention and disposal authority is to provide for the authorised disposal of State records which have been used as the input or source records for successful migration operations.

This authority is required because the process of migrating records yields two versions of the same record. The original record, known as the source record, continues to exist after a new version of it has been created by the migration process. In the majority of circumstances, there is no business need to retain both the source record and the new migrated version of the record. The normal administrative practice provisions of the *State Records Act 1998* which allow for the destruction of copies are not adequate for the authorisation of this form of disposal. While migration is in some respects a normal administrative practice it is also a complex process. It needs to be appropriately performed and comprehensively checked before the records created during the migration can be regarded as authentic copies of the original source records and before the source records can then be destroyed.

This authority therefore establishes conditions that must be met before public offices are authorised to destroy source records that have been successfully migrated.

1.2 What records does the authority cover?

This general retention and disposal authority applies to all source records that remain following the successful migration of records, irrespective of their date of creation. It applies to source records that have been migrated from all forms of business systems, not just those migrated from dedicated records management systems. It applies only to source records where it is the intention that the new migrated copy of the source record will be kept as the official record of business. It also applies equally to metadata records as to other forms of records. For example, a records management database that is used to control and describe a collection of paper files is a collection of metadata about the files. This metadata would serve as the source record for any migration of the database and the disposal of this source record metadata following its successful migration should be managed in accordance with the conditions specified in this authority.

1.3 Conditions for the destruction of records

To be able to destroy source records, a public office must ensure that the conditions for destruction described in this authority are met. These conditions are that:

1. The migration is planned, documented and managed
2. Pre and post migration testing proves that authentic, complete, accessible and useable records can and have been migrated

3. Source records are kept for a period of no less than six months following the successful migration of the records. In many cases their retention period will be longer than the mandatory six month minimum. The specific retention period will be based on organisational risk assessment.
4. For migrations within the public office, the target recordkeeping system meets the requirements of State Records' *Standard on Digital Recordkeeping* and preserves the migrated records as the official records of organisational business
5. For migrations to State Records, the migrations meet the conditions outlined in State Records' transfer requirements
6. The disposal of source records is appropriately documented

Guidance on complying with each of these conditions is provided in section 3 of this authority.

1.4 Records excluded from this authority

In addition to records that have been refreshed or replicated, the following specific record types are not covered by this authority:

- records copied for convenience or reference only
- encrypted records
- computer back-up tapes
- transcribed records
- analogue records being migrated to digital formats
- paper source records where their informational content has been transferred to a digital format.

Further information about these exclusions is provided in section 3 of this authority.

1.5 Status of this authority

This authority for the disposal of State records has been approved by the State Records Authority of New South Wales and may be implemented without further reference to State Records.

1.6 How long is this authority in force?

This authority will remain in force until it is superseded or withdrawn from use by State Records.

1.7 For more information

See section 3 of this authority, 'Guidelines for use', or contact State Records.

2 Records authorised for disposal

No	Record description	Disposal action
1	Records which have been used as the input or source records for successful migration operations.	<p>Source records may be destroyed if:</p> <ol style="list-style-type: none"> 1. The migration they are part of is planned, documented and managed 2. Pre and post migration testing proves that authentic, complete, accessible and useable records can and have been migrated 3. They have been kept for a period of no less than six months following their successful migration. In many cases their retention period will be longer than the mandatory six months minimum. The specific retention period will be based on organisational risk assessment. 4. For migrations within the public office, the target recordkeeping system meets the requirements of State Records' <i>Standard on Digital Recordkeeping</i> and preserves the records as the official records of organisational business 5. For migrations to State Records, the migrations meet the conditions outlined in State Records' transfer requirements 6. The disposal of source records is appropriately documented

3 Guidelines for use

3.1 About migration

What is migration?

Migration involves a set of organised tasks designed to periodically transfer records from one hardware or software configuration to another, or from one generation of technology to another, while maintaining the records' authenticity, integrity, reliability and useability. Data is generally inevitably changed by the migration process.

When migrating records, it is important that migration is performed on all aspects of a record – namely the record object and the metadata that supports it. Migration also can be performed on metadata only, for example, when the metadata that is used to manage hard copy records is moved from one system to another.

Migration is the key preservation strategy recommended in State Records' *Policy on digital records preservation*. It is a standard and often necessary practice, frequently driven by business needs to improve system functionality, that needs to be planned and managed appropriately to ensure the ongoing authenticity, accessibility and useability of digital records.

What is not migration?

For the purposes of this authority, the processes known as refreshment and replication are not regarded as forms of migration.

Refreshment is where data is transferred unchanged from one medium to another of the same type, for example, copying data from one CD-R to another. Replication is where data is transferred unchanged from one medium to another of a different type, for example, copying data from a hard drive to a CD-R.

Both these processes are forms of copying, not migration. While it is important to ensure that complete copies are made when refreshing or replicating, refreshment and replication are not subject to the stringent conditions outlined in this authority that apply to migrations. This is because refreshment and replication do not alter records in the same way that migration does. Migration as defined in this authority has the potential to have a significant impact on the accessibility and integrity of digital records and is therefore subject to the controls outlined in this authority.

Refreshment and replication should however always be performed with care and diligence. Appropriate checking should also be undertaken to ensure that the copying process was successful. Any superfluous copies of records that remain after refreshment or replication is complete may be disposed of in accordance with normal administrative practice.

Different types of migration covered by this authority

This authority authorises the destruction of the source records that remain following numerous different migration scenarios. These are:

<i>Migration from:</i>	<i>For example, in response to:</i>
<ul style="list-style-type: none">• one internal organisational	<ul style="list-style-type: none">• changing business needs that

<p>business system to another</p>	<p>lead to the adoption of a new business system</p> <ul style="list-style-type: none"> • technological changes that require the update of business systems • the need to transfer records from active business systems to long term storage systems • other internal and external drivers
<ul style="list-style-type: none"> • one organisation to another 	<ul style="list-style-type: none"> • administrative change that requires the transfer of functions or activities from one organisation to another • the adoption of shared service arrangements that require the transfer of records from one organisation to another • other internal and external drivers
<ul style="list-style-type: none"> • one organisation to State Records 	<ul style="list-style-type: none"> • requirements for the management of State archives, where State Records is required to take control and custody of State archives • other business drivers

Note that this authority does not authorise the disposal of records that have been transferred from hard copy, or paper, into a digital format. The disposal of paper records that have been scanned or digitised is covered by *General Retention and Disposal Authority – Imaged Records* (GDA24).

3.2 Conditions for the destruction of records

Because of its capacity to significantly alter record content and structure, migration is a high risk activity. Migration actions need to be well planned and effectively implemented in order for them to produce accurate versions of the source records that can be regarded for business and legal purposes as true copies of the original.

As a result of the high risk nature of migration activities, this authority outlines six conditions that must be met before source records can be destroyed. Implementing these conditions will help public offices to perform migration operations that produce accurate and authentic records. The conditions also seek to ensure that the migrated records are appropriately managed and that the migration process is adequately documented.

To be able to destroy source records, a public office must ensure that the conditions for destruction described in this Authority are met. These conditions are that:

1.	The migration is planned, documented and managed
----	--

2.	Pre and post migration testing proves that authentic, complete, accessible and useable records can and have been migrated
3.	Source records are kept for a period of no less than six months following their successful migration. In many cases their retention period will be longer than the mandatory six months minimum. The specific retention period will be based on organisational risk assessment.
4.	For migrations within the public office, the target recordkeeping system meets the requirements of State Records' <i>Standard on Digital Recordkeeping</i> and preserves the records as the official records of organisational business
5.	For migrations to State Records, the migrations meet the conditions outlined in State Records' transfer requirements
6.	The disposal of source records is appropriately documented

1. The migration is planned, documented and managed

<i>Minimum requirements:</i>	<i>This means that:</i>
The migration is planned	<ul style="list-style-type: none"> • all records requiring migration are identified • all records are complete, with accurate and appropriate metadata • where appropriate and where there is no longer a business need for them, records due for destruction are destroyed rather than migrated • the hardware, software and format requirements of the records requiring migration are understood • the essential characteristics of the records requiring migration are identified and can be replicated by the chosen migration strategy ¹ • metadata mapping between the original system and the target system is performed to ensure that all necessary metadata elements, their corresponding functionality and relevant business rules can be migrated between systems • for internal migrations and migrations to organisations other than State Records, the full

¹ Essential characteristics are the key characteristics that are critical to a record's meaning, use or organisational value. Essential characteristics will differ according to record type and the business purpose served by the record. For example, a report contains a map where colours are used to signify different agricultural areas. These colours have meaning – the report could not be interpreted accurately if these colours were not preserved. Therefore the colours are an essential characteristic of the report and any migration performed on this report must ensure that this essential characteristic is maintained.

	<p>functionality of the target system is identified and understood and the target system is configured appropriately to meet recordkeeping requirements</p> <ul style="list-style-type: none"> • the desired target state of the records post migration is identified • a migration method that will convert the records, including all metadata and essential characteristics, from their current state to the target state is developed
<p>The migration is comprehensive</p>	<ul style="list-style-type: none"> • all records requiring migration are migrated, including those that are stored online, near line, offline, in non active systems or secondary storage environments • the entire record, including all necessary metadata, is migrated • all essential characteristics have been preserved
<p>The migration is documented</p>	<p>The entire migration process and associated project planning should be documented. This could include:</p> <ul style="list-style-type: none"> • relevant research • all decisions, including decisions not to migrate certain metadata components of a record ² • risk assessments • the identified essential characteristics • the technical requirements of the original and target systems • the formal migration or transfer process • the date and time of the migration and all personnel involved • all system configurations, including metadata definitions and mappings • all testing • all reports that compare original system functionality to target system functionality • all sign offs • any data cleanup performed • any variations to plans • any necessary variation in records design, metadata, format or content that will or have resulted from the migration

2. Pre and post migration testing proves that authentic, complete, accessible and useable records can and have been migrated

² During the migration, public offices can decide not to migrate all metadata components of a record. This must only be the case for those metadata elements that have no ongoing business or accountability relevance for the organisation. Decisions not to migrate certain metadata elements should be fully considered and comprehensively documented.

<i>To be...</i>	<i>...the migrated record must be:</i>
Authentic	the product of well planned, comprehensive and successful migration processes
Complete	an accurate, legible reproduction of the source record in its entirety, including all its content, essential characteristics and all metadata identified as necessary
Accessible	available and readable to all those with a right to access it
Useable	able to serve the same business purposes as the source record and/or useable for ongoing reference

The testing to ensure that the migration process can deliver records that are authentic, complete, accessible and useable is divided into two phases: pre migration testing and post migration testing.

<i>Pre migration testing</i>	<i>Post migration testing</i>
<p>Once a migration strategy has been determined and all appropriate planning steps have been performed, a test migration needs to be performed on a small sample of duplicated records.</p> <p>The resulting migrated records need to be assessed and verified by relevant technical and business staff to ensure that they are authentic reproductions, are complete, accessible and useable and that the migration strategy is appropriate.</p> <p>Should adverse affects be noted in the migrated records, a revised migration strategy must be devised. This strategy should also be subject to pre migration testing.</p> <p>Pre migration testing needs to be documented. This documentation should provide the basis for the final migration plan.</p> <p>Once pre migration testing is complete, the pre migration testing and the finalised migration plan should be signed off by the Chief Information Officer or designated equivalent within the organisation.</p>	<p>Post migration testing must ensure that:</p> <ul style="list-style-type: none"> • all records identified for migration have been migrated • all necessary functionality and essential characteristics have been retained • users are satisfied with the authenticity, completeness, accessibility and useability of the migrated record <p>Post migration testing does not have to be performed individually on every record – testing at an aggregate level is appropriate. The number of records selected for testing needs to be appropriate either statistically or commensurate with the risk/business need for the records (for example, the number can be proportionate to the number of records migrated and should, where relevant, include different record types across a range of years).</p> <p>All testing must be documented.</p> <p>Once post migration testing is complete, the migration process should be signed off by the Chief Information Officer or designated equivalent within the organisation.</p>

3. Source records are kept for a period of no less than six months following their successful migration. In many cases their retention period will be longer than the mandatory six months minimum. The specific retention period will be based on organisational risk assessment.

Following their successful migration, source records must be kept for at least six months.

A retention period of six months allows time for any unforeseen issues associated with the migration that may emerge following post migration testing to be identified and rectified. Retaining the source records for at least this period will enable the migration to be repeated if it is discovered that some or all of the migrated records do not meet quality control standards or business requirements.

The six months retention period should begin to be calculated from the conclusion of successful post migration testing, where the migration and all outstanding issues associated with it have been signed off by the Chief Information Officer, or designated equivalent within the organisation.

In high risk scenarios it is likely that source records will need to be kept for longer than the minimum six months retention period required by this authority.

To determine whether source records need to be kept for more than six months and then to determine the specific length of the required retention period, public offices will need to use risk assessments to determine an appropriate retention period. These risk assessments should at a minimum consider:

- the business purpose of the records
- the risks associated with this business
- the potential business, financial and legal implications of the loss of or damage to the migrated records
- the size and complexity of the migration and the likelihood of problems associated with it
- the complexity of the records being migrated
- the capacities of the target system and the possibility that all aspects of this system and its impact on the records are not fully understood at the time of migration, and, where relevant,
- the nature of the metadata that is not being migrated.

Public offices should always err on the side of caution and if any problems or concerns with the migrated or transferred records are noted, such as corruption of portions of the record, or loss of information or distortions in the records caused by the new capacities or functionality of the target system, then the identified retention period must be extended by at least six months. Again, this additional retention period should begin to be calculated from the conclusion of successful post migration testing, where the repeated migration and all outstanding issues associated with it have been signed off by the Chief Information Officer or appropriate officer.

Retaining source records

It should be noted that this authority is not a requirement to destroy source records. In some situations, such as migrations between public offices, it may facilitate business processes for the transferring organisation to retain a reference copy of the source records for the length of their retention period, as specified in the relevant functional retention and disposal authority. Additionally, in high risk business environments, risk may best be mitigated by retaining source records as a

managed copy of the new official records. Cases, however, where public offices need to keep source records indefinitely should be very rare. Virtually all source records should be able to be destroyed after their retention period has expired.

4. For migrations within the public office, the target recordkeeping system meets the requirements of State Records' Standard on digital recordkeeping and preserves the records as the official records of organisational business

Under this authority, migrated versions of records are deemed to be official records. Procedures must be in place to ensure that the migrated form of the record is identified and managed as the official record of organisational business. All other versions of the record, including the source records, are copies and should not be regarded as the official record.

To preserve their authenticity, migrated records must immediately be captured and preserved in the most appropriate official recordkeeping system. It must be possible to demonstrate an unbroken chain of custody throughout the preservation process. This means that records should be taken from their parent system and migrated directly into their target system with as minimal intervention and time delay as possible. Any real or perceived lapse in the management of the record during the migration process may be seen as compromising its authenticity.

As official records, the migrated records should be managed in accordance with State Records' standards and requirements. To meet the conditions specified in this authority, migrated records must be managed in systems that meet the requirements of State Records' *Standard on Digital Recordkeeping*. These requirements are outlined in Appendix 1.

An official recordkeeping system can provide for the online or offline storage of migrated records, depending on the business requirements of the public office.

It can be difficult for a transferring organisation to ensure that this condition is met by the external organisation that is now responsible for the records. Therefore this is not a mandatory requirement for migrations between public offices. However it is critical in inter-agency migrations where records are transferred as a result of administrative change that both parties ensure that the target recordkeeping system meets the requirements of State Records' *Standard on digital recordkeeping*. All parties involved in the migration should work to ensure that the records are migrated and maintained in ways that best meet business, legal and accountability requirements, including the requirements of the State Records Act.

5. For migrations to State Records, the migrations meet the conditions outlined in State Records' transfer requirements

Section 29 of the State Records Act allows State Records to issue mandatory guidelines to govern the process of transferring State archives to State Records. When records are migrated to State Records, public offices must ensure that all conditions outlined in State Records' transfer requirements are met by the records being migrated.

6. The disposal of source records is appropriately documented

To comply with this condition, care must be taken to document and preserve destruction and transfer information after the source records themselves have been destroyed. (For further information about the appropriate means to destroy

records, see State Records' *Destruction of Records: A Practical Guide* and *Recordkeeping in Brief 51: Destroying digital records*.)

For migrations within the public office, the documentation of the destruction of the source record can take a range of forms, including:

- metadata at the aggregate or system level which states that the previous version of this record group or system was destroyed on the specified date, by the identified authorised officer, in accordance with the conditions outlined in this authority
- metadata at a more granular level that documents the destruction of the previous version of specific files in accordance with necessary disposal requirements
- a final migration report that outlines the destruction of source records, providing enough detail to identify all records or groups of records that have been destroyed.

The situation is different for source records that remain following migrations between one organisation and another or between one organisation and State Records. To document both the destruction of these source records and the migration/transfer of the records, a more detailed record needs to be retained. In addition to documenting the destruction of the source record and the authority for this destruction, a record must also be kept which identifies:

- the identity of all the records that have been transferred
- where the records have been transferred to, and
- the date of the transfer.

Whatever its form, documentation about records' disposal must be retained for significant periods of time. For example, for records that have been transferred to a successor organisation as a result of administrative change, the *General Retention and Disposal Authority - Administrative Records (GA28)*, requires that information about this transfer must be retained for a minimum of twenty years after the transfer (GA28, entry number 12.11.6). It also requires that details of records transferred to State Records must be retained on an ongoing basis within the organisation (GA28, entry number 12.11.3). The *General Retention and Disposal Authority - Administrative Records* also requires that any record documenting the implementation of disposal decisions should be maintained for a minimum of twenty years (GA28, entry number 12.11.1).

3.3 Records excluded from this authority

In addition to records that have been refreshed or replicated, the following record types are specifically not covered by this authority:

- records copied for convenience or reference only
- encrypted records
- computer back-up tapes
- transcribed records
- analogue records being migrated to digital formats
- paper source records where their informational content has been transferred to a digital format.

Records copied for convenience or reference only

This authority cannot be used to destroy official records after copies of these records have been made for convenience or reference purposes. Increasingly records are copied to different formats to facilitate web based access, downloading,

data sharing etc. This authority is not designed to cover the disposal of records that have been copied in this way.

Copied records of this type are generally authorised for destruction under the normal administrative practice provisions of the State Records Act (see State Records' guidelines on *Normal Administrative Practice* (Guideline 8, entry 3.1.5)) or may be referenced in relevant general and/or functional retention and disposal authorities. The original records that have been copied should be retained in accordance with the requirements of the relevant general or functional retention and disposal authority that applies to them.

Encrypted records

Encrypted records are usually created as a by-product of online authentication and security technologies such as Public Key Infrastructure. Encryption processes create a protected copy of a record that can be shared with other persons or organisations for information and business purposes. Records that have been encrypted are not covered by this authority.

The disposal of encrypted records is covered by the general and/or functional retention and disposal authorities that apply to the business documented within the encrypted record.

Computer backup tapes

Computer or system backup tapes are duplicate records, created as part of disaster management strategies on a daily or routine basis and overwritten frequently. Their purpose is to preserve organisational records in the event of system failure by creating a copy of all system data.

Disposal of back up tapes is not covered by this authority. Established routines for the destruction or overwriting of backups should be documented in disaster management or continuity planning policies and procedures.

Transcribed records

Transcription is used to copy the informational content of a record into a more accessible format. It creates a new record but both the original and transcribed record are generally kept as official records of the business. The source records for the transcription e.g. audio tapes, short hand notes, do not then fall within the parameters of this authority.

Disposal of the original source records after they have been transcribed should be covered by the relevant general or functional retention and disposal authority. Depending on the nature of the transcription process, and where this is supported by documented procedures and quality control processes, disposal of the original records may also be permitted under the normal administrative practice provisions of the Act (see State Records' guidelines on *Normal Administrative Practice* (Guideline 8, entry 3.1.4)).

Analogue records being migrated to digital formats

This authority is not intended to be used as a means to destroy analogue records that have been migrated to digital formats, such as analogue film or audio visual formats.

Analogue records involved in migrations of this type should be covered by relevant functional retention and disposal authorities.

Paper source records where their informational content has been transferred to a digital format

This authority does not apply to paper source records where the information contained in these records has been transferred into a digital format, for example information from an index card or data entry form that is input into a database.

The transfer of index card information in this way is covered by the *General Retention and Disposal Authority - Administrative Records* (see GA28, entry 12.9.4). Depending on the nature of the business process, and where this is supported by documented procedures and quality control processes, disposal of certain data entry input forms may also be permitted under the normal administrative practice provisions of the Act (see State Records' guidelines on *Normal Administrative Practice* (Guideline 8, entry 3.1.6)). Other information transfers of this kind should be covered by relevant functional retention and disposal authorities.

3.4 Relationship to other General Retention and Disposal Authorities

This general retention and disposal authority has similar requirements to those outlined in the *General Retention and Disposal Authority - Imaged Records*.

The *General Retention and Disposal Authority - Imaged Records* (GDA24) however covers different types of records. GDA24 covers (primarily) paper source records that have been imaged or scanned to create a digital copy and this authority covers records that have been created and maintained in digital formats and then migrated to a different digital format.

3.5 Destroying digital records

For more information on practical considerations of destroying digital source records that are authorised for destruction under this authority, public offices should refer to State Records' publications *Destruction of Records: A Practical Guide* and *Recordkeeping in Brief 51: Destroying digital records*.

Appendix 1: Requirements from State Records' *Standard on digital recordkeeping*

	Requirement
1	Minimum requirements for digital recordkeeping system functionality
1.1	<p>The public office must define the digital State records that it will make and keep.</p> <p><u>Note:</u></p> <p>The level of detail used by the public office to define the digital records to be made and kept should be adequate for implementation purposes and based on an assessment of the risk associated with the records and the business they document.</p>
1.2	<p>The digital State records that the public office has defined must be captured into an official digital recordkeeping system.</p> <p><u>Note:</u></p> <p>A digital recordkeeping system can be:</p> <ul style="list-style-type: none"> o a business system with recordkeeping functionality, or o a business system linked with a dedicated records management / information asset management system, or o a dedicated records management / information asset management system.
1.3	<p>Any digital recordkeeping system used for keeping official records must possess the following functionalities:</p> <ul style="list-style-type: none"> o capture read only versions of digital records o retrieve and present digital records in human readable form o restrict or permit access to records by specified individuals or groups o capture and manage the minimum required recordkeeping metadata as defined in this standard.
2	Minimum requirements for recordkeeping metadata
2.1	<p>Digital records must be captured into a digital recordkeeping system with:</p> <ul style="list-style-type: none"> o unique identifier o title o date of creation o who/what created the record o the business function/process it relates to o the creating application o record type (e.g. document / letter / memo / report / contract / fax / schematic / blog, or locally defined types).

	Requirement
2.2	<p>Any of the recordkeeping processes (listed below) that are performed on a record must be documented with:</p> <ul style="list-style-type: none"> ○ the date of the action ○ identification of who/what undertook the action ○ what action was undertaken. <p>The recordkeeping processes are:</p> <ul style="list-style-type: none"> ○ registration into a recordkeeping system ○ apply or change access rules ○ transfer of control ○ destruction ○ migration
2.3	<p>The transfer of control or destruction of records must be documented with:</p> <ul style="list-style-type: none"> ○ process metadata as above ○ an authorisation reference for the transfer or destruction (e.g. FA234 2.4.5; GA27 1.2.3; By court order etc.), and ○ in the case of transfer of the records, the name of the receiving organisation (e.g. Dept of X; State Records).
2.4	<p>At least the minimum required recordkeeping metadata as specified in this standard must be persistently linked with digital records and aggregations of digital records, including when they are transferred out of their original creating environment and through subsequent migrations.</p>
3	Minimum requirements for recordkeeping metadata management
3.1	<p>Recordkeeping metadata must be disposed of in accordance with the requirements of the State Records Act.</p>
3.2	<p>Metadata mappings from the minimum requirements of this standard to organisational digital recordkeeping systems must be documented and maintained, including any changes to these.</p>