Northern
Territory
Government

Guidelines for Disposing of Digital Source Records that have been Migrated

August 2013

NT Archives Service
NT Records Service

For information and advice, please contact
NT Records Service
Department of Corporate and Information Services
GPO Box 2391
Darwin NT 0801

Email:	NTG.RecordsPolicy@nt.gov.au
Telephone:	(08) 8924 3848
Facsimile:	(08) 8924 3880
Website:	http://www.nt.gov.au/dcis/info_tech/records_policy_standards/index.shtml

Table of Contents

1. Overview

The purpose of these guidelines is to provide advice when planning and implementing data migration projects where the digital platform or business system contains public records and what to do with residual digital source records.

Digital source records that have been migrated cannot be disposed of unless they have met certain criteria as outlined in accordance with the *Records Disposal Schedule for Digital Source Records that have been Migrated*. These guidelines need to be read in conjunction with that schedule.

These guidelines assume that records management staff are aware of all digital migration projects and are familiar with the *Information Act* and *Records Management Standards for public sector organisations in the NT*.

2. Definitions

Accessible – means able to be read or interpreted as having meaning.

Authenticity – means the digitized version replicates the attributes of the source records and can be proven to be what it purports to be.

Complete – complete records comprise contextual and structural data as well as content.

Digital Record – means any record that exists in binary form and that requires combinations of computer hardware and software to be read and understood.

Integrity – means the digitized version has the same degree of completeness as the source record so that it is able to be used for the same purposes as the source record.

Migrated Records - migrated records are those records resulting from the migration. They can also be called reproduction records.

Migration - the process of systematically moving records from one system to another, while maintaining the records authenticity, integrity, reliability and useability. The purpose of the migration is to preserve the integrity of the records and to retain the ability to retrieve, display and otherwise use them.

Reliability – means the contents of the digitized version has been created.

Source Records - the records being migrated.

Target Records – means the migrated record in the target platform.

Usability – means the digitized version of the source record can be located, retrieved, preserved and interpreted and maintains the contextual links of the source record to the records and activities for which the source record was created.

3. What records do these guidelines cover?

Advice in these guidelines applies to all digital source records that remain following the successful migration of records to the target system. Such as when:

- there are technology requirements that require the business system to be upgraded or the business system is being decommissioned
- changing business needs that lead to the adoption of a new business system
- machinery of government changes that require the transfer of functions of activities recorded in business systems from one public sector organisation to another.

It is important to know what records there are and describe them to ensure the digital records can be successfully maintained throughout the following migration process. Such as:

- content of the record (queries used so content can be retrieved)
- metadata of the record (who created the record, dates, records relationships etc)
- structure that allows the records to be accessible (containers, security, attachments etc)

Recordkeeping metadata is essential for preserving the authenticity of records.

These guidelines **do not** cover:

- technical advice on carrying out a data migration project
- any project management methodology adopted for the migration project
- digitisation of records from hardcopy format to digital format (refer to the *Records Disposal Schedule for Temporary Records that have been Digitised* – Disposal Schedule 2009/13*)*.

4. Migration processes

After determining what digital records require migration a documented and an approved plan needs to be developed.

The plan should include:

- objective
- outcomes
- stakeholders
- both the source and target systems
- formats of the digital records
- security requirements
- quality assurance procedures
- roll back strategy for mitigating risks to records in case an error occurs
- retention periods set
- disposal of source records

Refer to Appendix A for the Digital Source Records – Migration Project Checklist

4.1 Preparing digital records for migration

Before migration it is important to ensure that all records and metadata are as accurate and up-to-date as possible. This will increase the chances of a successful migration and improve the efficiency and quality of the migrated records.

Reviewing the record locations.	*Make sure that records are not assigned to people that have left the organisation.*
Ensure all records that require migration are in the source business system.	*Ensure records that need to be included are not sitting in shared drives, email accounts, personal drives, etc.*
Dispose of records that have met minimal retention requirements.	*This process will help with the quantity of records being migrated.*

4.2 Testing and validation

It is important to minimise any unanticipated and unacceptable results at the “go live” stage of the new platform.

Appropriate tests need to be undertaken to ensure the quality of the records. This will also assure all stakeholders that the digital records migrated are accurate, useable and authentic.

Testing methods could include:

- user acceptance testing scripts
- sampling a range of records
- validate a percentage of migrated records
- error message checking
- test the rollback strategy.

4.3 Migrating Records

The process of migration will involve export / import loading of data between the source platform and the target platform. Therefore the process must be undertaken with the minimum intervention and time delay as possible. Ultimately this will help prove the authenticity and reliability of the migrated records.

Once the migration process has been completed and testing and validating the data has been processed it is important to address all stakeholders and communicate how to move forward with regards to business rules for the source records to ensure they cannot be altered or are continually being used in business activity.

As official records, the migrated records should be managed in accordance with *Records Management Standards for public sector organisations in the NT*. 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 *Information Act*.

5. Quality assurance checks

There must be a plan for ensuring the quality of the migrated records to ensure they are authentic, useable and discoverable. Tasks include:

- compare number of records exported / imported match
- compare metadata and characteristics with source records and migrated records
- perform user acceptance testing and get target business area and technical staff to sign off the migration task.

Once post migration testing is complete, the migration process should be signed off by the relevant business unit manager and the organisation's Chief Information Officer or equivalent.

Refer to Appendix B for the Digital Source Records – Migration Testing and Validation Checklist.

6. Retention of source records

The *Records Disposal Schedule for Digital Source Records that have been Migrated* sets the minimum retention requirements of 12 months after the quality assurance plan has been signed off by an authorised delegate. The agencies however need to identify if the source records require further retention beyond the 12 months. A risk assessment should be established by the agency and consider the legal requirements and the business continuity issues that may influence the requirement to retain the source records for a longer period.

Risk assessment considerations include:

- business purpose, litigation potential and value of the records and the risks associated with this, including the potential business, financial and legal implications of any loss of trustworthiness or access
- level of assurance that "full and accurate" records have been achieved through the migration, including the completeness and authenticity of records
- level of assurance that the migrated records are being well managed in an approved electronic recordkeeping system

- thoroughness of the migration processes, including quality assurance processes and the size and complexity of the migration.

Source records must be stored and protected for this minimum retention period (12 months) to ensure that they remain authentic, useable and complete should there be a need for a “roll back” of migrated records.

Furthermore the source records must be protected from further business unit access to eliminate the possibility of their inadvertent use.

Agencies need to ensure that the digital source records are securely deleted once the approved retention period has expired so that they cannot be retrieved or recreated. (see section 8 of the guidelines).

Maintenance of two sets of records is not cost effective and can cause confusion over time as to which record is the official record of the business. Digital source records must be deleted once:

- the minimum retention period has been met
- quality assurance has been completed
- risk assessment procedures have been followed.

Agencies must take care to document and preserve destruction and transfer information after the source records themselves have been destroyed. A record must also be kept which identifies:

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

7. Recordkeeping documentation

The recordkeeping requirement for migrating digital source records is essential to justify business decisions and provide evidence of business transactions.

If migrated records were ever called into question during legal proceedings, it may be necessary to clarify that the migration process was reliable, and produced records that are authentic, reliable, usable, and complete.

Recordkeeping documentation can include:

- business case for the need to migrate digital records
- final migration plans and procedures
- risk assessment
- record testing and validation checks
- signed off quality assurance plans

8. Destroying digital records

For information on destroying digital source records that are authorised for destruction, refer to the *NT Government ICT Standard – Media Destruction*.

In HP TRIM the “remove document” function (NOT the “delete” function) can be used to destroy electronic records while retaining the record’s metadata.

9. Acknowledgement

The NT Records Service acknowledges the following authorities that have been used as a foundation for this guideline:

- Queensland State Archives – *Migrating Digital Records – a guideline for Queensland public authorities*
- Queensland State Archives – *General Retention and Disposal Schedule for Digital Source Records*
- State Records Authority of New South Wales – *General Retention and Disposal Authority, Source Records that have been Migrated (GA33)*

APPENDIX A: Digital Source Records – Migration Project Checklist

Stage One	**Migration Project Initiation** The initial stage of high-level scheduling and resource planning for the project.	- Business drivers - Project briefs - Project plans - Risk assessments - Roles and Responsibilities - Stakeholder Communication Plan
Stage Two	**Determine what is to be migrated** The stage of the project when the scope of the migration is being established.	- Business process analysis - List of records / record groups identified - Digital source records retention obligations - Records metadata
Stage Three	**Determine where and how to migrate** The stage when it is established the method for the migration to the target systems	- Verifying target systems recordkeeping capabilities - Making file/record format decisions - Establishing the migration approach
Stage Four	**Ensuring Quality** The stage when quality assurance, including testing and validation processes, are identified, planned and undertaken.	- Preparing records for migration - Ensuring records and metadata are up-to-date - Complete sentencing projects prior to migration - Data cleansing plan - Testing and validation documentation including outcomes
Stage Five	**Performing Migration** The stage documenting the migration to extract, export, transfer and add import records into the target system.	- Testing roll back strategy - Recordkeeping plan during cut over period - Migration of records - Quality assurance of migration results
Stage Six	**Post Migration** The final stage of the project	- Quality Assurance procedures to be signed off - Verifying conditions for disposal of source records - Disposal of digital source records in accordance with the *Records Disposal Schedule for Digital Source Records that have been Migrated* - Stakeholder communication and moving forward plan including business rules and procedures

APPENDIX B: Digital Source Records – Migration Testing and Validation Checklist

Check accuracy of the content and metadata of the records.

For example:

- Expected fields are populated with data (eg. mandatory values)
- Field values are in keeping with expected lengths and valid date ranges
- Values are populated with expected data types (eg numeric, alphanumeric, date, etc)
- Metadata values remain accurate, particularly those such as the date of creation and dates which trigger disposal countdowns
- Accurate metadata about the migration process itself is captured

Check for completeness that all records identified for migration, have been migrated and that the completeness of the records themselves is verified.

For example:

- Numbers of records remains the same
- Linkages/relationships between metadata and records are maintained
- Results of standard reports and searches are repeatable, consistent, and accurate

Check for maintenance of the integrity and authenticity of the records.

For example:

- All agreed characteristics of the records as previously identified for migration during the planning process are maintained
- Any errors or corruption during transmission are flagged, eg as identified through checksums – an IT computational process that can highlight errors that might have occurred during the migration process.

Check for meaningfulness and the access and usability of the records.

For example:

- Real time checks of sample records to ensure they remain readable and understandable
- After roll-out the system /platform is stable and operating within acceptable error log

Check the reliability of the systems/including functionality, processes and integrated systems / peripherals.

For example:

- After roll-out, the system is stable and operating within acceptable error log margins that have been established in collaboration with IT colleagues.