



Information
Communication
and Technology

NSW Department of Corrective Services

Procedure – Disposal of Imaged Records

Prepared by: Mira Milczarek
Manager, Information Management Framework

Doc. No. 2006-?-PRC-v1.0

Release Date 23 /07/07

Copy Number 1

DOCUMENT CLASSIFICATION

Public

Acceptance Notice

This is a controlled document. All copies of this document preceding this release are obsolete and should be destroyed. This document has not been released for use until authorised by the Assistant Director, IC&T, Standards, Information Security & QA and approved by Executive Director, IC&TD or his delegate.

QA Authorised: Date: / /2007
 Al Benazzi, Assistant Director, IC&T, Standards
 Information Security & QA

Approved: Date: 23/07/2007
 Wayne Ruckley, Executive Director Information Communication & Technology

Revision History

Version Number	Date	Revision history
1.0	06/10/06	Initial Draft
1.0	23/07/07	Approval

Associated Documents/References

- AS ISO 19005-1:2005 – Document Management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF / A-1)
- GDA 24 – Imaged Records
- Electronic Transactions Act 2000
- Evidence Act 1995

- The State Records Act, 1998
- Freedom of Information Act 1989
- Privacy and Protection of Personal Information Act 1998
- Protected Disclosures Act 1994 No 92
- Crimes Act 1900 No 40
- Public Sector Employment and Management Act 2002 No 43
- Queensland State Archives - Guideline for the Digitisation of Paper Records, Version 2, April 2006
- Archives Office of Tasmania, Recordkeeping Advice No. 3, Day Batching of Source Records, Issued 13 July 2005
- The Legal Admissibility of information stored on Electronic Document Management Systems, or How to make the Law Love your Image, A paper by The Calderson Consultancy Principal, Michael J. Steemson presented to the 4th International Records Management Congress in Edinburgh, Scotland, April 29th 1998
- ISO IEC 27001-2005 Information Technology – Security Techniques – Information Security Management Systems

Acronyms & Abbreviations

DCS	Department of Corrective Services
IC&TD	Information Communication & Technology Division
CIMS/TRIM	Corporate Information Management System
PDF	Portable Document Format
TIFF	Tagged Image File Format
PPI	Pixels Per Inch

Distribution

Copy Number	Version Number	Date Issued	Issued To
1			

Table of Contents

1. Identification.....	5
2. What this procedure does.....	5
2.1. Purpose.....	5
2.2. Requirements for this Procedure.....	5
3. What this procedure is.....	5
3.1. Description.....	5
3.2. Audience.....	6
3.3. Approach.....	6
3.4. Inputs.....	6
4. Definition.....	7
4.1. Capture Requirements.....	7
4.2. Identification and consistent Classification.....	7
5. Ownership.....	7
5.1. Roles and Responsibilities.....	7
5.1.1. Role of the Director Information Management.....	7
5.1.2. Role of the Manger Operations, Information Management Branch.....	7
5.1.3. Role of the Archives Manager.....	8
5.1.4. Role of the Manager Information Management Framework.....	8
5.1.5. Role of Unit/Branch Manager.....	8
5.1.6. Role of the Information Management Officer.....	8
5.1.7. Role of the Records Representative.....	8
5.1.8. Role of the Record Keeper.....	9
6. Sensitivity.....	9
6.1. Security Controls.....	9
6.1.1. Security Levels.....	9
6.2. ‘Read Only’ controls.....	9
7. Quality.....	10
7.1. Technical Considerations.....	10
7.2. Standard Format.....	10
7.3. Image enhancement.....	11
7.4. Disposal Authority.....	12
7.5. Conditions for the disposal of Imaged Records.....	12
7.6. Disposal of Imaged Records.....	14
7.6.1. Disposing of imaged records before GDA 24 was issued.....	15
7.7. Retention of Imaged Records.....	15
7.8. Quality Control - Validation.....	15
7.9. Batching.....	16
7.10. Quality Control/Imaging Process.....	16
8. Accessibility.....	17
Appendix 1 – Imaging - Checklist.....	19
Appendix 2 – Declaration of Compliance – Digitisation Disposal Certification.....	23
11. Glossary.....	25

1. Identification

Procedure number

?

ITIL Processes Supported

N/A

Point of Reference

Manager Information Management Framework
Archives Manager
Operations Manager, Information Management Branch

2. What this procedure does

2.1. Purpose

The purpose of this procedure is to establish sound records management practices and a consistent approach with regard to the destruction of certain original records and State Records which have been successfully captured/copied using microfilming or through digital processes such as scanning.

2.2. Requirements for this Procedure

AS ISO 19005-1:2005 Document management – Electronic document file format for long-term preservation

3. What this procedure is

3.1. Description

The department has a firm commitment to transitioning to complete electronic record management to realise enhanced efficiencies and quality in information management. The digital scanning of paper records is an important transitioning technology. This procedure recognises the need to manage this growing practice.

This procedure guides decision making and processes with respect to destroying original records that have been appropriately digitally captured or copied. A primary requirement for the proper destruction of imaged records is to ensure that all legal requirements are met including validation that the digitisation process has captured a true and accurate

record of the original, and that permanently valuable records are identified and preserved. Records must only be destroyed in accord with corporate policy and procedures and therefore allow the department to account for its records.

3.2. Audience

This procedure shall be adhered to by all DCS staff who intend on using scanning/imaging technology to create and capture corporate records, however the procedure is targeted at managers of business processes supported by digital scanning.

3.3. Approach

The construct of this procedure references the DCS Information Management Characteristics outlined in Table 1 below to ensure consistency in the development and management of DCS Information Assets. Each of these characteristics is designed to facilitate the effective collection, storage, access, use and eventual disposal of information and its constituent data.

Table 1: Information Management Characteristics

Information Framework Characteristic	
Definition	The explicit identification and consistent classification and description of information holdings
Ownership	Management of the rights and responsibilities of agencies as custodians of government owned information
Sensitivity	Management and security of sensitive information to protect privacy and confidentiality Information Security Management System Dimension: Confidentiality
Quality	Documentation of quality, accessibility, completeness, currency, consistency and integrity of information Information Security Management System Dimension: Quality – integrity
Accessibility	<ul style="list-style-type: none"> ▪ Management of information to provide affordable access through an open communications network. ▪ Effective and reliable internal access and interagency exchange and affordable access to the public for relevant information. Information Security Management System Dimension: Accessibility – availability

3.4. Inputs

- Corporate Information Management System (CIMS)

4. Definition

4.1. Capture Requirements

All imaged records must be captured in CIMS. The Corporate Information Management System will keep essential recordkeeping metadata that will facilitate the records preservation and retrieval.

4.2. Identification and consistent Classification

Each imaged record must be stored in the CIMS using the accepted Corporate Classification Scheme naming protocols.

Scanning of images/records must be done using DCS approved software and hardware as specified in the IC&T Service Catalogue in order to capture technical metadata such as image resolutions, bit depths, compression and file formats. Without this associated metadata for imaged records DCS will not be able to prove that the image is a true and exact copy of an original (after disposal of the physical record). And therefore the disposal of the original is not permitted

For more information on Classification rules refer to the [Information Management Framework – Corporate Records Procedures Manual](#) section 11. Classification Scheme Titling and the [Corporate Classification Scheme](#)

5. Ownership

5.1. Roles and Responsibilities

5.1.1. Role of the Director Information Management

The Director of Information Management sets the strategic direction for the Department in the area of optimising the value of its information resources and aligning the collection, storage, access, use and disposal practices and supporting systems within best practice to facilitate information to the business in the form and at the time it is required. The Director of Information Management manages the Department's web presence, corporate reporting, information exchange and records practices in ensuring the availability, confidentiality and integrity of DCS information.

5.1.2. Role of the Manger Operations, Information Management Branch

The Manger Operations, Information Management Branch manages and provides

high-level advice regarding the development and implementation of the Corporate Records Program and ensures the provision of accurate, cost effective and responsive access to administrative and operational records. The Manger Operations, Information Management Branch ensures that the Information management Branch provides a high level of service and an effective logistics function with respect to physical records and mail.

5.1.3. Role of the Archives Manager

The Archives Manager manages the operation of the Corporate Records Repository, local operations units and contracted storage facilities, ensuring the safety, security, accessibility, reliability, integrity and usability of repositied information stock.

5.1.4. Role of the Manager Information Management Framework

The Manger Information Management Framework promotes effective and compliant Information Management practices throughout DCS by ensuring the accuracy, integrity and usability of information resources.

5.1.5. Role of Unit/Branch Manager

Ensures digital and disposal procedures are developed and maintained in accord with these guidelines and Records Management Policy.

5.1.6. Role of the Information Management Officer

Information Management Officers are employed within the Corporate Information Management Branch to provide high level customer service and support to Records Representatives and other Corrective Services staff on record keeping practices in maintaining the integrity of the Department of Corrective Services Information Management Framework.

5.1.7. Role of the Records Representative

Records Representatives are nominated staff within units/divisions who have more extensive record keeping responsibilities than Record Keepers. Each operational area will need to nominate at least one Records Representative.

Records Representatives –

- Conduct regular documental validation checks on digitised records.
- Manage and maintain the day to day records management processes and operations within their area, and
- Support Record Keepers within their area on records management matters such as the registration of files in CIMS; the conduct of disposal process for files; the creation of physical files and the conduct of a census for files etc.

5.1.8. Role of the Record Keeper

Everyone who creates and uses records day-to-day is a Record Keeper and needs to understand the Record Keeper's responsibilities, such as requesting and creation of files, tracking files and attaching documents to files.

6. Sensitivity

6.1. Security Controls

All staff are responsible for applying the appropriate security controls to scanned images to protect the sensitivity of corporate information. Access to records/images within the CIMS is directed by the security level afforded to particular files and through the use of Groups and Caveats.

Staff are reminded that all original (physical) documents inherit the same security level as the imaged/scanned record. Access to Highly Protected, Protected and In Confidence records shall be limited to staff with the appropriate security clearance and shall be secured when unattended. In areas where many people have access to filing cabinets, and/or compactuses, controls shall exist or be established to limit access to authorised users.

6.1.1. Security Levels

All files shall have one of the following security levels:

- Highly Protected
- Protected
- In-Confidence
- Unclassified
- Public

For more information on security protocols for electronic/imaged records refer to the [Information Management Framework – Corporate Records Management Procedures Manual](#) section 5. Security

6.2. 'Read Only' controls

Staff are required to use only approved image formats.

DCS approved image formats include Portable Document Format (PDF) and Tagged Image File Format (TIFF) for scanned/imaged records as these provide 'read only' controls ensuring data integrity and accessibility.

7. Quality

7.1. Technical Considerations

Departmental staff must observe the following recommended technical guidelines when scanning records/images into CIMS:

Recommended Resolutions (minimum)		
Document Type	Page size	Resolution
Standard text documents	Up to A3	No less than 300 PPI
Oversized documents, e.g. maps	Larger than A3	No less than 200 PPI
Photographs	6"x4"	600 PPI
	7"x5"	430 PPI
	9"x6"	300 PPI
Digitising at a higher resolution than recommended may be necessary if there is a requirement to enlarge the image for use or to capture highly detailed paper originals.		
Recommended bit Depths		
Document Type	Bit Depth	
Black and White text only	1-bit bi-tonal	
Text with some colour	8-bit colour	
Text with shades of grey	4-bit or 8-bit grey	
Colour drawings/presentations/graphics	8-bit colour	
Black and white photographs	8-bit grey	
Colour photographs	24-bit colour	
If imaging a document containing a mix of the above, such as a black and white page which includes a colour photograph then the highest colour depth should be used to capture it, e.g 24 bit colour.		
Recommended Compression		
<p>Lossless compression <u>must be used where possible</u> as it provides file size reduction while being able to reproduce an exact, true and accurate digital copy of the image document/record.</p> <p>Lossy compression will not be permitted for records authorised for early disposal as some loss of data may occur resulting in the accuracy of the image being called to question. Lossy compression may only be used on some file types when the original document/record is being retained.</p>		
Note: DCS Branches/Units should combine reference to these guidelines with their own testing on typically digitised documents prior to selecting which resolutions to use.		

7.2. Standard Format

The standard format for DCS imaged records is PDF (with the exception of TIFF format for invoice scanning).

PDF is a digital format that has become the standard for the exchange and storage of data. PDF files may be created natively in PDF form, converted from other electronic formats, or digitised from paper, microfilm or other hard copy formats.

TIFF is a digital format that is widely supported. TIFF files are commonly used in desktop publishing, faxing, 3-D applications and medical imaging applications.

Scanning of images/records must be done using DCS approved software and hardware as specified in the IC&T Service Catalogue.

Note: TIFF lacks the compression and bit depth combinations (other than bi-tonal images) to suit other document types, particularly greyscale and colour documents. File sizes can potentially become very large, affecting accessibility and storage. JPEG may be implemented with TIFF or PDF to overcome the size issue but it uses a lossy compression scheme (unsuitable for file disposal). PDF covered by ISO 15930-1:2001 and the De facto standard. TIFF covered by De facto standard. See www.archives.qld.gov.au/publications/digitisation/DigiGuideline.pdf Recommended File formats pg. 38.

Document Type	File Format
Text document with only one colour of text	TIFF PDF
Document with watermarks, grey shading, grey graphics etc.	PDF
Document with discrete colour used in text or diagrams, etc	PDF
Black and white photographs	PDF
Colour photographs	PDF

7.3. Image enhancement

Any image enhancement undertaken to imaged files must be noted and registered in the notes section of the document type. This includes enhancements such as:

- Despecking
- Deskewing
- Crop Boarder
- Invert Images
- Smoothing/sharpening
- Colour correction, etc.

7.4. Disposal Authority

Prior to destruction of Imaged Records, staff must ensure that records considered for destruction under **GDA 24 – General Retention and Disposal Authority – Imaged Records**, are covered by a current, approved General or Functional Disposal Authority.

GDA 24 operates together with other disposal authorities in that the record’s retention period must be known before it can be dealt with after imaging. It is important to ensure that any records that are being considered for destruction under GDA 24 are covered by a current, approved General or Functional Retention and Disposal Authority.

7.5. Conditions for the disposal of Imaged Records

To legally destroy imaged records, staff must ensure that the conditions for destruction are first met. These are:

Documentation		
1	Do you have a local procedure for scanning documents?	
	If...	Then...
2	Yes	Go to step 4
3	No	<p>Create local procedure for scanning documents. Include:</p> <ul style="list-style-type: none"> • Unit/Branch • Type of records scanned • Machine used • Hardware maintenance • Design of Imaging system e.g. vendor documentation on how the system works what controls it has and what image integrity it has • Validation • Protocol for which file scanned documents are to be attached to • Protocol for filing, storing, preparing for archive and/or destruction. <p>See template in appendix 1 – Imaging – Checklist</p>

Assessment		
	If...	Then...
4	You can identify an appropriate disposal class for the record in a current, approved General or Functional Retention and Disposal Authority	Go to step 5
5	The record is not of a type listed in the 'Exclusions' in GDA 24	Go to step 6
6	Under the record's original disposal authorization, the record is authorised for eventual destruction	<p>The original may be destroyed after copying, provided the conditions listed in GDA 24 are met. These are:</p> <ul style="list-style-type: none"> • All requirements for retaining originals have been assessed and fulfilled • Copies are made which are authentic, complete and accessible • Copies are kept for the authorised retention period • Originals are kept for the approved length of time after copying for quality control purposes.
7	Under the record's original disposal authorisation, the record is required as a State archive	<p>Determine whether the record was created or received before or after January 1, 2000:</p> <ul style="list-style-type: none"> • If it was created or received from Jan 1 onwards, the original may be destroyed after copying, provided the conditions are met • If the record was created or received prior to Jan 1, 2000, then permission is not given to destroy the original after copying under GDA 24. Contact State Records if you wish to seek special permission.

Where originals are destroyed under GDA 24, the image copies must be retained for the full retention period specified for the originals.

Where originals are not authorised for destruction under GDA 24, they should be registered in CIMS for management and retrieval purposes and retained for their full retention periods.

Disposal of any records under GDA 24 should be in accordance with current DCS Disposal procedures this includes:

- Listing of records for disposal/destruction on the Information Management Archival/ Destruction Certificate or directly into CIMS/TRIM in the Box Record Type, under Notes/Box Contents (refer to below procedures for more information).
- Identifying the disposal authority/ies used.
- Gaining approval for destruction from your Governor/Branch head, the Manager Operations, Corporate Records Branch and the Director of Information Management.
- Forwarding original (batched) documents in a registered Archival Box to the Corporate Records Repository for destruction.

Note: A Declaration of Compliance – Digitisation Disposal Certification (see appendix 2) must be completed by the Director Information Management or delegate prior to disposal of original records scanned into CIMS. This will follow and be listed after review of the local procedures submitted by the process owner (Appendix 1).

Refer to the [Information Management Framework – Corporate Records Management Procedures Manual](#) section 12 Disposal and the Self-Help Records Archival/Disposal Procedures for Users without CIMS access and the [Self-Help Records Archival/Disposal Procedures for Users with CIMS access](#).

7.6. Disposal of Imaged Records

Prior to disposal of imaged records, staff must ensure that no special requirements exist to retain the records in its original format. Special requirements for DCS may include:

- A special legislative requirement for a record to be retained in its original format – for example, for display
- A business rule that relies on distribution of a hard copy record around the organization for annotation or sign-off
- The possible use in the future of graphic materials eg. Posters, designs, photographs, brochure for display

- Customer expectations that they will be able to access certain records relating to them in their original formats.

Staff responsible for imaging or imaging projects should document the results of their assessment of such requirements for retaining originals, and obtain approval for the destruction of records from a senior manager before forwarding to the Corporate Records Repository for destruction

Refer to Appendix 1 for Imaging - Checklist

7.6.1. Disposing of imaged records before GDA 24 was issued

Provided that the originals are eligible for destruction under the rules in GDA 24, they may be destroyed. Staff should ensure that images are authentic, complete and accessible, and that any other conditions for destruction have been met. If the documentation is inadequate then the originals should be retained. Remember, originals identified as State archives created or received prior to January 1, 2000 are not eligible for destruction after copying under GDA 24.

7.7. Retention of Imaged Records

Where the original State record is legally destroyed, the image copy becomes the official State record. Therefore, it must be retained for the period specified in the disposal class under which the original record was covered.

Note: Considerations must include the verification that the technology to retain all types of state record relating to specific software will be available, if not it may be necessary to produce a list of all files required by State Records that are kept by DCS and retain physical files of these records.

7.8. Quality Control - Validation

The quality control and validation process is the single most important consideration in transitioning from paper to digital. There is both an individual and corporate obligation to render true and accurate copies of the originals.

Original records that have been imaged must be kept for 3-6 months prior to authorised destruction, for quality control purposes and as a safeguard in case of loss of images in the copying or registration process.

Records/documents must:

- Be carefully prepared e.g. ensure documents are not folded, obscuring

information prior to scanning- **Staff**

- Be stored in Corporate Information Management System (CIMS) – **Staff**
- Be quality checked after scanning to ensure that they are an exact copy of the original – **Staff** (audit)
- Have preservation measures and monitoring in place to protect the optical media on which the images are stored from deterioration – **IC&T**
- Be retained (originals only) for 3-6 months for quality control/disaster recovery purposes – **IM branch**.

7.9. **Batching**

It is recommended that DCS staff use Batch storing of original documents. Batch storing provides an easy method of checking that:

- All required activity has been performed
- Any anomalies have been noted
- Appropriate quality procedures have been completed &
- Records of any exception process have been made

Original documents which have been scanned must be stored in Archive boxes which have been registered in CIMS. This ensures that the disposal of imaged records under GDA 24 is authorised and documented.

When batching scanned records, care must be taken to ensure that originals **not authorised** for destruction after imaging are preserved.

- Originals must be kept for quality control purposes for 3-6 months
- The person doing the scanning must be aware of the exclusions from the GDA 24, so that these originals can be retained and managed separately.
- Ensure the imaged copies are being registered into the CIMS and properly sentenced using the appropriate disposal authority.

7.10. **Quality Control/Imaging Process**

When scanning/imaging documents a register of events will be kept. The following information must captured during the scanning registration process –

- Identify the person who performed the scanning (captured automatically in CIMS/TRIM)
- Type of material scanned (e.g. paper document, microfilm etc) (in CIMS/TRIM)

Document Type)

- Extract of post-scanning processes (e.g. de-skewing, de-specking etc.) performed (captured by operator in the notes section)
- Date and time of scanning (captured in CIMS/TRIM automatically)

It is important that any anomalies during the scanning process are acknowledged and registered, either with a view to correcting them or merely making note of them. This way, when the accuracy or the contents of the Corporate Information Management System is challenged in court, the department will be able to identify where mistakes were made.

8. Accessibility

All imaged copies of records must be captured in the CIMS. DCS will ensure that planning for long term accessibility of images is documented by:

Keep copies of...	...to show...
Organisational policy and procedures that apply to the making and keeping of digital images of records, including superseded versions of the policies/procedures	<ul style="list-style-type: none"> • Which classes or records are routinely imaged, which are authorised for destruction • The rules that apply to staff in making and keeping the images • The normal period of time DCS keeps originals for quality control purposes • What checking and verifying and other quality control processes are in place
Documentation of the design of the imaging system	<ul style="list-style-type: none"> • Data compression methods and formats have been chosen to suit the nature of the records and DCS' requirements • That image enhancement techniques adopted do not substantively alter the records
Documentation of assessments carried out of any requirements to retain records in original format from legislative or business requirements	<ul style="list-style-type: none"> • Identification of any special reasons why originals should be retained by DCS • Identification and consideration of risks of not keeping some records in their original formats • Conditions attached to destroying originals under GDA 24 have been met

<p>Planning documents relating to ensuring the long term accessibility of the image copies</p>	<ul style="list-style-type: none"> • The measures are in place to ensure long term accessibility to the images • The digital records are managed in appropriate and trustworthy systems
<p>Disposal documentation (eg. Metadata in records system indicating date and time of destruction and authorisation).</p>	<ul style="list-style-type: none"> • Records are disposed of (both original hardcopy and image copies) in an authorised and accountable way.

Appendix 1 – Imaging - Checklist

9.

Imaging – Checklist

Unit/Branch Name:

**Make and Model of
Machine used to
image record/s:**

**Type of Document/s
Imaged. (see
Section 7.2 of this
procedure for
examples):**

1. Preparation **Completed/Checked**

- 1.1 Documents are not folded prior to scanning
- 1.2 All obstructions and/or any additional material like “post-it” notes, tags etc. have been removed.

2. Metadata Capture in CIMS

TIP: You may not see the date, time and creator (person who performed scanning) in the registration window (‘New Document Type’ window) during the registration process. To check if these fields have been captured highlight/click on the document number (after registration has been completed) and check the metadata section (lower half of the results window).

- 2.1 Date and time of scanning captured in CIMS
- 2.2 Name of person performing the scanning captured in CIMS
- 2.3 Type of material scanned has been identified in the ‘Document Type’ section of the ‘New Document Type’ window

3. Security

- 3.1 Imaged Records have appropriate security applied
- 3.2 Imaged Records are in DCS approved formats (PDF and TIFF) and are set as Read Only (no changes can be made electronically to the imaged record).

4. Quality Check

- 4.1 Imaged copy has been checked to ensure it is a true, complete and accurate representation of original
- 4.2 Any alterations e.g. deskewing and/or anomalies with the imaged Record/s have been acknowledged and registered in the ‘New Document Type’ Notes metadata field.

5. Batching/Storing of Original imaged Records

- 5.1 CIMS/TRIM document number of scanned document recorded on original record
- 5.2 Original records authorised for disposal under GDA 24 placed in CIMS registered Archival Box, for Quality control/Disaster Recovery purposes (for a period of three (3) to six (6) months).
- 5.3 Original records not authorised for destruction under GDA 24

placed in Administration File and stored.

6. Disposal

For more information on the Disposal of DCS Records and/or completing a Archival/Disposal Certificate please see the Information Management Framework – Corporate Records management Procedures Manual section 12 Disposal and the Self-Help Records Archival/Disposal Procedures for Users without CIMS access.

- 6.1 Records are no longer required for Quality Control/Diaster Recovery purposes
- 6.2 Original Records requiring destruction have been listed on the Archival/Disposal Certificate
- 6.3 Appropriate disposal Authority/ies have been identified
- 6.4 Approval for destruction has been obtained from Governor/Branch Head
- 6.5 Approval for destruction has been obtained from Manager, Operations, Information Management Branch and Director, Information Management
- 6.6 Records have been collected by Corporate Records Repository or an approved service provider for destruction

Name of person imaging records:	Signature of person imaging records:
Date:	
Name of Branch Head	Signature of Branch Head
Date:	

If you have any queries regarding the disposal of imaged records, please contact repository staff on phone number 02 9289 5540.

Appendix 2 – Declaration of Compliance – Digitisation Disposal Certification

10.

Declaration of Compliance – Digitisation Disposal Certification

This form must be signed by the Director Information Management

Prerequisites (tick box to confirm agreement)

I confirm that the Department of Corrective Services has developed and implemented the following:

1. Corporate Classification Scheme
2. Authorised Retention and Disposal Schedule/s
3. Electronic Document and Records Management System
4. Published recordkeeping policies and procedures
5. Appropriately skilled staff for the digitisation and recordkeeping program

Compliance criteria (tick box to confirm agreement)

I further certify that the classes of records proposed for early disposal (see Archival Disposal Authority) have been assessed in accordance with the GDA 24 – Imaged Records and the DCS Disposal of Imaged Records Procedure and that the following criteria have been met:

1. The classes listed for disposal are covered by a current, approved General or Functional Disposal Authority.
2. The records are not of a type listed in the ‘Exclusions’ section in GDA 24.
3. Under the record’s original disposal authorisation, the record/s are authorised for eventual destruction.
4. Any record/s required as a State Archive have been preserved.
5. No format-specific retention requirements apply to the records, which are not overridden by section 20 of the Electronic Transactions Act 2001.
6. A risk assessment has shown that there is low risk of the original records being required in legal proceedings or for other purposes.

Compliance conditions (tick box to confirm agreement)

I further certify that the scanning/imaging systems and processes used to capture digitised copies of official records are compliant with the following conditions:

1. That policies and procedures have been developed and implemented by DCS covering:
 - Roles and responsibilities for the selection, digitisation and management of digitised records, and the secure management and disposal of originals
 - Technical specifications for digitisation
 - Capture of technical imaging metadata, and
 - Quality assurance procedures
2. That the system has been designed with adequate physical and other security safeguards to ensure the public records remain inviolate and can only be changed in an authorised manner.
3. That the system has appropriate audit trails in place.
4. That appropriate metadata is captured and maintained, including that:
 - Audit records are retained as recordkeeping metadata
 - The mandatory recordkeeping metadata elements are captured and maintained in accordance with the Recordkeeping Metadata Standard for Commonwealth Agencies, including the allocation of retention and disposal actions.
 - Technical imaging metadata is generated and captured at the point of digitisation.
5. That the system is covered by business continuity and disaster recovery plans.
6. That DCS has a published migration strategy in place to ensure that public records are not placed at risk of loss through technological obsolescence.

Signed _____ Date _____

(Director Information Management)

11. Glossary

<i>Definition</i>	<i>Meaning</i>
Archiving	The processes of boxing, listing, sentencing and transferring semi-active records to an onsite storage facility or an offsite storage provider.
Data Storage Device	Data Storage Device means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device
Disposal	Disposal means destruction, abandonment, transfer of ownership, transfer out of NSW, damage or unauthorised alteration.
Disposal Authorities	Pre-determined guidelines showing what records can be destroyed and when these records may be destroyed by specifying a retention period; and what records cannot be destroyed, that is must be retained permanently. These records are known as State Archives.
Documents	Structured units of recorded information, published or unpublished, in hard copy or electronic form, and managed as discrete units in information systems.
Electronic Communication	<ol style="list-style-type: none"> 1. A communication of information in the form of data, text or images by means of guided or unguided electromagnetic energy, or both, or 2. A communication of information in the form of sound by means of guided or unguided electromagnetic energy, or both, where the sound is processed at its destination by an automated voice recognition system
Electronic Mail	A computer based message sent over a communications network to one or more recipients, which may be transmitted with attachments such as electronic files containing text, graphics, images, digitised voice or computer programs.
Electronic Records	Records communicated and maintained by means of electronic equipment.
Ephemeral records	Records of little value that only need to be kept for a limited or short period of time. Ephemeral records have no continuing value to the organisation and, generally, are only needed for a few hours or a few days.
Files	A file is a collection of documents that show organisational activities through an identifiable sequence of transactions
Information	Information in the form of data, text, images or sound
Information Management	The discipline and organisational function of managing records to meet operational business needs, accountability requirements and community expectations.
Information system	A system for generating, sending, receiving, storing or otherwise processing electronic communications.
Recordkeeping	Making and maintaining complete, accurate and reliable evidence of

	business transactions in the form of recorded information.
Records	Recorded information, in any form, including data in computer systems, created or received and maintained by an organisation or person, the transaction of business of the conduct of affairs and kept as evidence of such activity.
State Archives	Records that are permanently retained for their historical, research and intrinsic value and are transferred to State Records
State Record	Any record, made and kept, or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public office, or for the use of a public office.

END OF DOCUMENT