TAHO
Tasmanian Archive + Heritage Office

State Records Guideline No 21

Approved destruction methods for State Records

Department of Education
LINC Tasmania

Tasmania
Explore the possibilities

Table of Contents

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History

Build Status

Version	Date	Author	Reason	Sections
2.0	28-05-2015	Christine Woods	Template	All
1.0	08-04-2013	David Bloomfield	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
All	All	Document imported into new template.

Issued: August 2013

Ross Latham
State Archivist

1 Introduction

Destruction of records applies to records in all formats including digital or electronic records (records communicated or maintained by means of electronic equipment).

1.1 Purpose

The purpose of this guideline is to set down those methods that are approved by the State Archivist for the destruction of temporary State records.

The *Archives Act 1983* stipulates that a government employee, or any other person MUST NOT dispose of records of any type without the written authority of the State Archivist and requires agencies to preserve records until they are dealt with under the Act. This guideline provides further information about the obligations flowing from these requirements.

Users of this Guideline MUST also refer to the Tasmanian Government Information Security Manual[1].

1.2 Authority

This guideline is issued under the provisions of Section 10A of the *Archives Act 1983*. Guidelines issued by the State Archivist under this Section set standards, policy, and procedures relating to the making and keeping of State records. This section also requires all relevant authorities to take all reasonable steps to comply with these guidelines, and put them into effect.

Keyword	Interpretation
MUST	The item is mandatory.
MUST NOT	Non-use of the item is mandatory.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
RECOMMENDS RECOMMENDED	The item is encouraged or suggested.

'MUST' and 'MUST NOT' statements are highlighted in capitals throughout the Guideline. Agencies deviating from these MUST advise TAHO of the decision to waive particular requirements.

Agencies deviating from a 'SHOULD' or 'SHOULD NOT' statement MUST record:

[1] http://www.egovernment.tas.gov.au/__data/assets/pdf_file/0015/155202/Tasmanian_Government_-_Information_Security_Policy_Manual.pdf

- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- the date at which the decision will be reviewed, and
- whether the deviation has management approval.

Agencies deviating from a 'RECOMMENDS' or 'RECOMMENDED' requirement are encouraged to document the reasons for doing so.

2 What you must do before you can destroy a record

If you intend to destroy a State record and it is not described in an authorised Disposal Schedule, you MUST contact the Tasmanian Archive and Heritage Office to gain a Destruction Authority. If the record is described in an authorised Disposal Schedule, you MUST make sure that the minimum retention period for that record has expired. You MUST also check:

- information that does not fit that sentence has not been added to the record
- that the record is not required or likely to be required in judicial proceedings, by government inquiries or investigations, by applications for access under Right to Information, or by applications for access under other legislation

Once you have decided which records are due for destruction you MUST record this process in your Register of Records Destroyed. Further guidance on how to complete this Register can be found in Recordkeeping *Advice No. 9 Disposal of Scheduled Records.*

3 How do I destroy a record

To destroy a State record you MUST make them unreadable and irretrievable.

3.1 Physical records

The only approved methods for destroying physical records such as papers, photographs and films is shredding or pulping.

Burning records is NOT RECOMMENDED and should only be used as a last resort if there is no environmentally friendly method of destruction available. Records should be burned in accordance with any environmental guidelines and local burning restrictions. Densely packed paper does not burn well, so burning should be undertaken in an industrial facility (not in a backyard incinerator).

3.2 Digital records

Deletion is not destruction and does not meet the requirements for destruction of State records. When digital records are deleted it is only the pointer to the record (such as the file name and directory path) that is deleted. The actual data objects are gradually overwritten in time by new data. However, until the data is completely overwritten, there remains a possibility that the information can be retrieved. Methods of destroying digital records include:

- digital file shredding
- degaussing – the process of demagnetising magnetic media to erase recorded data

- physical destruction of storage media – such as pulverisation or shredding
- reformatting – if it can be guaranteed that the process cannot be reversed

To ensure the complete destruction of a digital record, all copies MUST be found and destroyed. This includes removing and destroying copies contained in system backups and offsite storage. The decision of how to destroy your digital records should be based on a risk assessment.

3.3 How do I make sure records are properly destroyed?

When you destroy records, it is RECOMMENDED that you are there to see the destruction is carried out by the contractor at least on the first occasion that you use a particular service provider.

The contractor MUST always supply you with a certificate of destruction. If records that were supposed to be destroyed are subsequently found, the certificate is evidence that the contractor was at fault, not your own agency. It is RECOMMENDED that you request that the certificate of destruction includes the method of destruction used by the contractor.

The contractor can either collect records from your office for destruction, or you can deliver the records to them. It is RECOMMENDED that a closed truck be used whenever possible. However, if there is no alternative and the contractor can only provide an open truck, ensure that the load is secured by a cover. Sensitive and confidential records SHOULD only be conveyed in a closed and lockable vehicle. Furthermore, records deemed to be confidential SHOULD be transported in lockable wheelie bins.

The Tasmanian Information Security Policy Manual outlines the different levels of security that SHOULD be assigned to agency records. Agencies SHOULD use this as their template when assessing the appropriate manner for managing destruction of records:

Record security classification and corresponding minimum AALs (Access Assurance Levels)	Approved methods of destruction according to the Manual
PUBLIC AAL-0 No Assurance	• Paper waste: no specific requirements (as per Section 6.1 of this Guideline). • Electronic media and equipment: may contain information of other classifications, therefore as per Section 3.3.3 of the 'Tasmanian Information Security Policy Manual' (p54).
UNCLASSIFIED AAL-1 Minimal Assurance	• Paper waste: destruction by shredding is optional (as per Section 6.1 of this Guideline). • Electronic media and equipment: as per Section 3.3.4 of the 'Tasmanian Information Security Policy Manual' (p54).

Record security classification and corresponding minimum AALs (Access Assurance Levels)	• Approved methods of destruction according to the Manual
IN CONFIDENCE AAL-2 Low Assurance	• Paper waste: destruction by cross-cut shredding. • Electronic media and equipment: as per Section 3.3.4 of the 'Tasmanian Information Security Policy Manual' (p54).
PROTECTED AAL-3 Moderate Assurance	• Paper waste: secure destruction using a Class B shredder rated by the Australian Government Security Construction and Equipment Committee. • Electronic media and equipment: as per Section 3.3.4 of the 'Tasmanian Information Security Policy Manual' (p54).
HIGHLY PROTECTED AAL-4 High Assurance	• Paper waste: secure destruction using a Class B shredder rated by the Australian Government Security Construction and Equipment Committee. • Electronic media and equipment: as per Section 3.3.4 of the 'Tasmanian Information Security Policy Manual' (p54).

3.4 Disposal of ICT equipment

When disposing of ICT equipment, agencies MUST sanitise any media in the equipment that is capable of storing records, remove the media from the equipment and dispose of it separately or destroy the equipment in its entirety. Agencies MUST remove labels and markings indicating the classification, code words, caveats and owner details to ensure the sanitised unit does not display indications of its prior use. Only once the media in ICT equipment has been sanitised or removed can the equipment can be considered sanitised.

3.5 Sanitising network devices

Routers, switches, network interface cards and firewalls contain memory which is used in the operation of the network device. Agencies SHOULD reset the device and load a dummy config (or equivalent) to exercise the device memory and provide a read back to verify the reset was successful.

3.6 Media that cannot be sanitised

Attempts to sanitise media may sometimes be unsuccessful, in which case the media MUST be destroyed. Additionally, some types of media cannot be sanitised and therefore MUST be destroyed. Agencies MUST destroy the following media types prior to disposal, as they cannot be sanitised:

- microfiche
- microfilm
- optical discs
- printer ribbons and the impact surface facing the platen
- programmable read-only memory
- read-only memory
- faulty or other types of media that cannot be successfully sanitised.

		Destruction Method				
		Hammer Mill	Disintegrator	Grinder/Sander	Cutting	Degausser
ITEM	Electrostatic memory devices	Yes	Yes	Yes	No	No
	Magnetic floppy disks	Yes	Yes	No	Yes	Yes
	Magnetic hard disks	Yes	Yes	Yes	No	Yes
	Magnetic tapes (includes audio and video tapes)	Yes	Yes	No	Yes	Yes
	Optical disks	Yes	Yes	Yes	Yes	No
	Semiconductor memory	Yes	Yes	No	No	No

4 Definitions

agency - is used in this guideline to refer to all agencies, authorities, statutory offices, departments, councils and other organisations that are subject to, and defined in, the *Archives Act 1983*.

destruction – is the rendering of a record as unreadable and irretrievable.

record - is a document or an object that is, or has been, made or kept by reason of any information or matter that it contains or can be obtained from it or by reason of its connection with any event person, circumstance, or thing.

sanitisation - is the process of removing information from media. It does not automatically change the sensitivity or classification of the media, nor does it involve the destruction of media.

State records - records of State government agencies/departments, State authorities, or local authorities. These public bodies are defined in Section 3 of the *Archives Act 1983*.

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Acknowledgements

- Department of Premier and Cabinet, *Information Security Policy Manual (April 2011)*[2]
- Department of Defence, Intelligence and Security *Australian Government Information Security Manual – Controls (September 2012)*[3]
- National Archives of Australia *Compliant destruction of Australian Government records*[4]

[2] http://www.egovernment.tas.gov.au/__data/assets/pdf_file/0015/155202/Tasmanian_Government_-_Information_Security_Policy_Manual.pdf
[3] http://www.asd.gov.au/infosec/ism/
[4] http://www.naa.gov.au/records-management/agency/keep-destroy-transfer/destroying-records/index.aspx