

State Records Guideline No 13

Certification for secondary storage providers

Table of Contents

I Introduction	
I.1 Purpose.....	4
I.2 Authority.....	4
I.3 Overview	4
2 How to gain and renew certification.....	5
3 Background Information	6
4 Certification checklist	15
References.....	20
Appendix: List of ISO Storage Standards	21

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
4	9 June 2016	David Bloomfield	Update of documents required for renewal of certification and update of the site inspection checklist. Also clarification that no storage areas on site can be used to store anything that could harm the records.	4 Certification Checklist
3	13 August 2015	Sam Foster-Davies	New Template	All
2	25 November 2014	David Bloomfield	General update of Guideline	2 How to gain and renew certification 3 Background information 4 Certification Checklist
1	27 June 2013	David Bloomfield	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
Certification checklist	4	Disaster management plan, Staff employment agreement, Contract template for government customers and Inspection reports now required for certification renewal.
Site Inspection	4	General revision of Site Inspection checklist.

I Introduction

I.1 Purpose

The purpose of this Guideline is to detail the requirements that MUST be met by a commercial storage provider for certification as an Approved Secondary Storage Provider (ASSP) for State records.

I.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:

- 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.

I.3 Overview

Agencies MUST NOT use a commercial storage provider unless that provider is currently certified as an ASSP. Certification MUST be approved by the State Archivist and MUST be renewed every two years. Once a supplier has received certification a certificate will be issued to the provider and this will be recorded on the GISU website.

If an agency has records stored with a non-approved provider, the agency MUST take all reasonable steps to locate an ASSP in their region and, once the current contract with their existing supplier has terminated, arrange all agency records to be relocated to the ASSP's storage facilities.

2 How to gain and renew certification

There are many issues to be addressed for a secondary storage provider to gain certification as a storage facility for State records. To gain certification, the items listed in the Certification checklist (pp.15-19) **MUST** be produced and/or inspected at the time of appointment with a TAHO staff member. Further information and assistance in how to gain certification can be obtained by contacting us at:

Government Information Strategy Unit - Tasmanian Archive and Heritage Office
91 Murray Street
Hobart 7000
Email GISU@education.tas.gov.au
Phone 6165 5581

A certified provider **MUST** contact TAHO if at any time they undertake any changes that impact on their ability to meet the requirements outlined in this Guideline.

A provider's certification is current for a period of two years. Prior to its expiry the provider **MUST** arrange a meeting with an officer from TAHO to renew their certification. For a certification renewal, only those items marked (*) in the Certification Checklist (pp15-19) **MUST** be produced and/or inspected. However, in the event a provider builds or acquires additional premises, it **MUST** go through the original certification process even if it is a previously approved provider.

3 Background Information

Where an agency decides to use the services of a commercial storage provider, both parties **MUST** articulate their roles and expectations in the service contract.

The service contract **MUST** clearly state the obligations and responsibilities of the agency and the storage provider. This **MUST** include coverage for liability and insurance. Such issues may be determined by the value of the records (reflected by their security and sensitivity attributes, vital record status and retention period) and the anticipated cost of recovery and restoration in the event that records are damaged during storage or transit.

The terms and conditions of contractual arrangements will vary in each case, but **MUST** reflect the requirements to be met for certification as an ASSP detailed in this Guideline.

The tables below list the requirements and examples of evidence for meeting each requirement.

Authorisation

<i>Principle: all State records <u>MUST</u> be stored in conditions that are authorised by the State Archivist</i>	<i>Examples of Evidence</i>
1. Storage areas and facilities which store State records MUST be certified by the State Archivist, and any conditions or limitations noted in the certification.	<ul style="list-style-type: none"> TAHO certification issued by the State Archivist of an ASSP for commercially operated storage areas and facilities used by the agency.

Inspection

<i>Principle: areas and facilities used for the storage of State records <u>MUST</u> be regularly inspected for compliance.</i>	<i>Examples of Evidence</i>
2. Storage areas and facilities MUST be inspected and assessed regularly for compliance with this Guideline.	<ul style="list-style-type: none"> ASSP certification that the secondary storage provider is compliant. Confirmation on the TAHO website that the secondary storage provider is ASSP certified.

Inspection (contd)	Examples of Evidence
<p>3. Random checks of information contained within a sample of records in storage areas and facilities SHOULD occur at least every six months to identify signs of pest infestation, computer viruses, data corruption or information loss.</p>	<ul style="list-style-type: none"> • Risk register with entries regarding high risk records in storage areas or facilities. • If storing digital records, inspection logs with details of checks conducted to detect signs of data corruption or information loss. • Procedures to check integrity of records containers when retrieved from storage areas. • If storing digital records, disaster management plans which include procedures for the recovery of lost information.

Location and Construction

Principle: State records <u>MUST</u> be stored in areas which are located away from known and unacceptable risk.	Examples of Evidence
<p>4. The location of each storage area or facility SHOULD be subjected to a risk assessment to identify and mitigate possible risks to the preservation of and access to State records stored there, and the results SHOULD demonstrate that the level of risk is low.</p>	<ul style="list-style-type: none"> • Internal risk assessment reports which identify and evaluate risks to record storage areas and facilities and how they will be mitigated.
<p>5. Storage facilities MUST be assessed as being compliant with the Building Code of Australia and associated codes.</p>	<ul style="list-style-type: none"> • Certificates of occupancy which demonstrates that the facility meets Building Code requirements, including relevant fire-resistance levels.
<p>6. Storage areas for all records (hardcopy or digital) MUST be protected from fire, water influx, and have an integrated pest management system in place.</p>	<ul style="list-style-type: none"> • Storage plan detailing design measures and safeguards implemented in record storage areas and facilities to protect records from fire, water influx (from above, below or through walls or openings) and vermin. • Internal risk assessment reports which detail risk mitigation strategies for hardcopy record storage areas and facilities.

Location and Construction (contd)	Examples of Evidence
<p>7. Storage areas and facilities for magnetic storage media MUST be protected from magnetic fields, including (but not limited to) high intensity electro-magnetic fields (e.g. high voltage power lines), lightning conductor systems, electric generators and motors and electrical wiring.</p>	<ul style="list-style-type: none"> Internal risk assessment reports which detail how magnetic storage media has been protected from the effects of magnetic fields.
<p>8. All storage areas on site MUST NOT be used to store anything that could harm the records (such as chemicals or flammable liquids).</p>	<ul style="list-style-type: none"> Policy and procedures which confirm that equipment or substances which pose a risk to records were not present in all record storage areas and facilities.
<p>9. Storage areas and facilities MUST be designed to minimise the impact of sunlight and UV light on records.</p>	<ul style="list-style-type: none"> Internal risk assessment reports which detail how the impact of sunlight and UV light on records has been minimised.
<p>10. Storage areas and facilities MUST have sufficient floor loading capacity to safely support the maximum volume of records, their containers and any furnishings or equipment.</p>	<ul style="list-style-type: none"> Certificates of occupancy specifying floor loading capacity. Structural engineer's report confirming storage areas and facilities have sufficient floor loading capacity to support records and equipment when at full capacity.

Preservation and Safety

<p>Principle: State records <u>MUST</u> be stored in conditions that ensure their preservation for as long as the records are required, and the safety of the people handling the records.</p>	<p>Examples of Evidence</p>
<p>11. Technology used for the storage of digital records <u>MUST</u> be chosen to ensure the records (and their contextual metadata) are preserved and accessible.</p>	<ul style="list-style-type: none"> • Assessment reports which identify appropriate storage technology for digital records.
<p>12. Temperature and humidity levels within storage areas <u>MUST</u> be monitored for stability, and action taken to minimise any significant fluctuations.</p>	<ul style="list-style-type: none"> • Assessment reports which identify appropriate storage conditions for records in storage facilities. • Inspection logs which demonstrate monitoring of temperature in storage areas.
<p>13. State digital, photographic or other sensitive media types being transferred to or from cool or cold storage areas <u>SHOULD</u> be acclimatised in accordance with the relevant International Standard before being introduced to a new temperature zone (see Appendix for list of relevant ISO standards)</p>	<ul style="list-style-type: none"> • Storage plan which includes the use of acclimatisation zones outside cold storage areas (typically used for digital and photographic media). • Record retrieval and returns procedures which require the use of acclimatisation zones for cold storage.
<p>14. Shelving and handling equipment <u>MUST</u> be appropriate for the format of the records. Wooden shelving <u>SHOULD</u> be avoided as it can release harmful vapours, can contribute to the spread of fire and may harbour insects.</p>	<ul style="list-style-type: none"> • Assessment reports which identify appropriate storage and handling equipment for records. • Visual inspection by TAHO staff • Inspection logs which demonstrate that shelving and handling equipment are being used appropriately.

Preservation and Safety (contd)	Examples of Evidence
<p>15. Individual shelves <u>MUST</u> be able to safely support the maximum volume of records and their containers. If boxes are stacked without shelving, they <u>SHOULD NOT</u> be stacked more than four high and <u>SHOULD</u> be in a staggered formation, like brickwork, to avoid caving in boxes on the bottom row.</p>	<ul style="list-style-type: none"> • Assessment reports which identify appropriate shelving for records. • Visual inspection by TAHO staff
<p>16. Containers used to store records <u>MUST</u> be clean, in good condition, and appropriate to record weight, size and format to assist with the preservation of the records they contain.</p>	<ul style="list-style-type: none"> • Record storage procedures which cover the selection and appropriate use of containers. • Visual inspection by TAHO staff

Identification and Control

Principle: State records <u>SHOULD</u> be stored using systems that enable the records to be retrievable.	Examples of Evidence
<p>17. Systems for the physical and intellectual control of State records within storage areas and facilities <u>MUST</u> be implemented to track the locations and movements of records.</p>	<ul style="list-style-type: none"> • Clauses in contracts and service level agreements that require the control of records. • System manuals which detail the physical control of records. • System manuals which detail the intellectual control of records. • Database identifying the location of digital records on digital media, and the location of the digital media itself.
<p>18. Procedures for retrieval, handling and returning of records within storage areas or facilities <u>SHOULD</u> be developed and communicated to those authorised to access the records.</p>	<ul style="list-style-type: none"> • Records management procedures for the retrieval, handling and returning of records in storage. • Service level agreements with clients which covers the retrieval, handling and returning of records in storage.

Security

<p>Principle: State records <u>MUST</u> be protected from theft, misuse and inappropriate or unauthorised access or modification, whilst they are being stored, or in transit to and from a storage facility or area.</p>	<p>Examples of Evidence</p>
<p>19. Storage areas and facilities <u>MUST</u> be protected from unauthorised access and destruction.</p>	<ul style="list-style-type: none"> • Policies and procedures which include details of security measures implemented to protect record storage areas and facilities. • If storing digital records, ICT security and access control model which includes details of network and computer security controls to protect digital records from viruses and unauthorised access. • Inspection logs which demonstrate that security measures are working correctly.
<p>20. State records in transit to or from storage areas and facilities <u>MUST</u> be protected from unauthorised access and destruction (includes transmission via physical and technological means).</p>	<ul style="list-style-type: none"> • Policies and procedures which include details of security measures implemented to protect records while in transit. • Procedures which detail how to keep records secure during transfer (e.g. locking courier satchels).
<p>21. Records <u>MUST</u> be handled and stored in compliance with the requirements of their security classification and mandatory requirements as outlined in the ‘Tasmanian Government Information Security Policy Manual’(see pp22-28, 53 of the Manual)</p>	<ul style="list-style-type: none"> • Policies and procedures which include details of appropriate handling and storage of security classified records. • Information security procedures which detail how to store information with different security classifications

Maintenance

<p>Principle: A maintenance program, including regular inspection, review and monitoring, <u>MUST</u> be in place for all areas and facilities that store State records.</p>	<p>Examples of Evidence</p>
<p>22. An ongoing maintenance program <u>MUST</u> be implemented to identify, assess and mitigate risks to the security and preservation of State records in storage areas and facilities.</p>	<ul style="list-style-type: none"> • Maintenance program for storage areas and facilities which details activities to be undertaken to mitigate risks to the security and preservation of State records (e.g. clearing gutters, upgrading hardware and software). • Risk register which includes entries regarding risks to storage areas and facilities.
<p>23. Storage areas and facilities (including shelving and handling equipment) <u>MUST</u> be kept clean and in good working order.</p>	<ul style="list-style-type: none"> • Storage plan which includes a program of regular cleaning and maintenance. • Visual inspection by TAHO staff • Inspection logs which demonstrate that shelving and handling equipment have been regularly checked and maintained. • Pest management and fire servicing logs which demonstrate that checks have been performed.
<p>24. Software on online or near-line computer systems used to store digital records <u>SHOULD</u> be supported and maintained by people with the appropriate skills and competencies.</p>	<ul style="list-style-type: none"> • Records management or Information & Communications Technology (ICT) policy which requires computer systems to be supported and maintained. • Service level agreements or maintenance and support contracts for computer systems which are current.

Disaster Prevention and Recovery

<p><i>Principle: An up-to-date disaster preparedness, management and recovery program <u>MUST</u> be in place for all areas and facilities that store State records.</i></p>	<p><i>Examples of Evidence</i></p>
<p>25. A disaster preparedness, management and recovery program for records within storage areas and storage facilities <u>MUST</u> be reflected in the contract the provider has with the agency.</p>	<ul style="list-style-type: none"> • Disaster preparedness, management and recovery plan which defines responsibilities and includes contact details of specialist disaster recovery companies. • Contract between provider and agency that indicates there is a disaster preparedness, management and recovery program for records within storage areas and storage facilities.
<p>26. Records in storage areas or facilities and in transit <u>MUST</u> be insured (either by the provider or the agency) for recovery and restoration in the event of a disaster.</p>	<ul style="list-style-type: none"> • Disaster management plan includes agency insurance policy details, insurance coverage for record recovery and restoration activities and claims procedures. • Copies of agency or courier certificates of insurance.
<p>27. Fire detection and extinguishing equipment <u>MUST</u> be installed and maintained in all storage areas and facilities in accordance with relevant Australian standards by a qualified contractor.</p>	<ul style="list-style-type: none"> • Fire safety logs or inspection reports showing that smoke detectors meet requirements of AS 1670 and fire extinguishers, hose reels and hydrants meet the requirements of Part E of the Building Code of Australia.
<p>28. Equipment, supplies and information required to assist with the recovery of records after a disaster <u>MUST</u> be set aside in designated areas within or near storage areas and facilities.</p>	<ul style="list-style-type: none"> • Disaster preparedness, management and recovery plan which details required recovery supplies and their location. • Visual inspection by TAHO staff • Contact lists for disaster recovery organisations. • Disaster bin content lists and inspection checklists.

Disaster Prevention and Recovery (contd)	Examples of Evidence
<p>29. Staff members responsible for the recovery of records following a disaster <u>MUST</u> receive training in carrying out their allocated responsibilities.</p>	<ul style="list-style-type: none"> • Disaster preparedness, management and recovery plan which includes staff training activities. • Reports regarding disaster training exercises. • Staff training records which demonstrate that all relevant staff have recently received training in disaster recovery activities.

Document to be produced	Evidence to be shown	Checked OK	Comment
6. Insurance renewal (if provider includes insurance coverage for the customer)*	<ul style="list-style-type: none"> detailing insurance coverage for record recovery and restoration activities and claims procedures 	<input type="checkbox"/>	
7. Documentation of general training exercises for staff*	<ul style="list-style-type: none"> training in retrieval, handling and returning of records to storage training in security procedures for storing records requiring different security classifications training in disaster preparedness, management and recovery program for records within storage areas and storage facilities. manual handling certificates 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
8. Staff employment agreement *	<ul style="list-style-type: none"> covering confidentiality requirement 	<input type="checkbox"/>	
9. Contract template for government customers *	<ul style="list-style-type: none"> clause requiring insurance cover with the provider OR requiring proof the agency has own insurance cover. clause stating that intellectual control of the customer's records remains with the State of Tasmania. clause detailing options in the event the customer fails to pay for storage <u>without</u> resorting to the destruction of the customer's records. clause that requires in the event the provider goes into receivership that arrangements be made for ongoing access to the records by the customer 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Document to be produced	Evidence to be shown	Checked OK	Comment
10. Fire safety logs or inspections reports*	<ul style="list-style-type: none"> showing that smoke detectors meet requirements of AS 1670 and fire extinguishers, hose reels and hydrants meet the requirements of Part E of the Building Code of Australia. 	<input type="checkbox"/>	
11. Inspection reports *	<ul style="list-style-type: none"> showing up to date pest inspection/eradication Showing up to date gutter cleaning 	<input type="checkbox"/> <input type="checkbox"/>	
12. Assessment reports (digital records only)*	<ul style="list-style-type: none"> identifying appropriate storage technology for digital records 	<input type="checkbox"/>	

Site Inspection

Subject	Checked OK	Comment
1. Does the site have suitable metal shelving or racking?	<input type="checkbox"/>	
2. Is the bottom shelf above floor level?	<input type="checkbox"/>	
3. Does the site use forklifts for moving boxes? If so do relevant staff have forklift licences?	<input type="checkbox"/> <input type="checkbox"/>	
4. Are ladders single or step? Do they have locking devices? Do they have signage to indicate how high you can climb? Do they have a standing platform? If so, do they have a rail or enclosure?	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Subject	Checked OK	Comment
<p>5. Is there an external security fence?</p> <p>Is it complete and in good condition?</p> <p>Is it at least 6 feet high?</p> <p>Is it lockable? If lockable, what kind of lock is on it?</p>	<p><input type="checkbox"/></p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p>	
<p>6. Does the building have security locks on windows, doors, roller doors?</p>	<p><input type="checkbox"/></p>	
<p>7. Does the building have monitored alarm systems?</p>	<p><input type="checkbox"/></p>	
<p>8. Are there security cameras?</p>	<p><input type="checkbox"/></p>	
<p>9. Are there fire extinguishers?</p> <p>Are there suppression systems?</p>	<p><input type="checkbox"/></p> <p><input type="checkbox"/></p>	
<p>10. Is the storage area clean and tidy?</p>	<p><input type="checkbox"/></p>	
<p>11. Is the storage area located away from areas of known risk such as kitchens, bathrooms, overhead plumbing etc?</p>	<p><input type="checkbox"/></p>	
<p>12. Is the storage area protected against vermin infestation?</p> <p>If so how is this done?</p>	<p><input type="checkbox"/></p>	
<p>13. Is the guttering cleared regularly?</p> <p>If so who does this and is it documented?</p>	<p><input type="checkbox"/></p>	

Subject	Checked OK	Comment
<p>14. Is the storage area and all neighbouring storage areas only used for records storage?</p> <p>If not please elaborate?</p>	<input type="checkbox"/>	
<p>15. Are the records stored away from direct sunlight?</p>	<input type="checkbox"/>	
<p>16. Are the boxes in good condition and stacked appropriately? (ie stacked no more than 4 high)</p>	<input type="checkbox"/>	
<p>17. Is the temperature monitored?</p> <p>If so, what action is taken to modify the temperature if required?</p>	<input type="checkbox"/>	
<p>18. In the case of digital and photographic records, is there an acclimatisation zone outside cold storage areas?</p>	<input type="checkbox"/>	

References

Australian Building Codes Board, *Building Code of Australia, volumes one and two of the National Construction Code* <http://www.abcb.gov.au/about-the-national-construction-code/the-building-code-of-australia>

Department of Premier and Cabinet, *The Tasmanian Government Information Security Policy Manual* (April 2011)

http://www.egovernment.tas.gov.au/standards_and_guidelines/tasmanian_government_information_security_framework

National Archives of Australia, *Standard for the Physical Storage of Commonwealth Records* (December 2002)

http://www.naa.gov.au/Images/standard_tcm16-47305.pdf

Public Records Office Victoria, *Certification Checklist – Approved Public Record Office Storage Supplier (APROSS)*

(PROV PRO39 2011) <http://prov.vic.gov.au/government/standards-and-policy/all-documents/pro-39>

Public Records Office Victoria, *Specification 1: Agency Custody Storage* (PROS 11/01 2011)

<http://prov.vic.gov.au/wp-content/uploads/2011/05/1101s1.pdf>

Public Records Office Victoria, *Specification 2: State Archives POD Storage* (PROS 11/01 2011)

<http://prov.vic.gov.au/wp-content/uploads/2011/05/1101s2.pdf>

Appendix: List of ISO Storage Standards

The list below is not exhaustive but covers some of the most common media types. Providers **SHOULD** identify all media types to determine which ISO storage standards will be of relevance. The International Organization for Standardization may have additional standards covering other media types of relevance.

Magnetic Tape

International Organization for Standardization 2000, *ISO 18923 Imaging materials - Polyester-base magnetic tape - Storage practices*, ISO, Geneva, Switzerland.

Multiple Media

International Organization for Standardization 2006, *ISO 18934 Imaging materials - Multiple media archives - Storage environment*, ISO, Geneva, Switzerland.

Optical Disc

International Organization for Standardization 2008, *ISO 18925 Imaging materials - Optical disc media - Storage practices*, ISO, Geneva, Switzerland.

Paper & Parchment

International Organization for Standardization 2003, *ISO 11799 Information and documentation - Document storage requirements for archive and library materials*, ISO, Geneva, Switzerland.

Photographic Film

International Organization for Standardization 2002, *ISO 18928 Imaging materials - Unprocessed photographic films and papers - Storage practices*, ISO, Geneva, Switzerland.

International Organization for Standardization 2000, *ISO 18920 Imaging materials - Reflection prints - Storage practices*, ISO, Geneva, Switzerland.

International Organization for Standardization 2000, *ISO 18918 Imaging materials - Processed photographic plates - Storage practices*, ISO, Geneva, Switzerland.

International Organization for Standardization 2000, *ISO 18911 Imaging materials - Processed safety photographic films - Storage practices*, ISO, Geneva, Switzerland.