



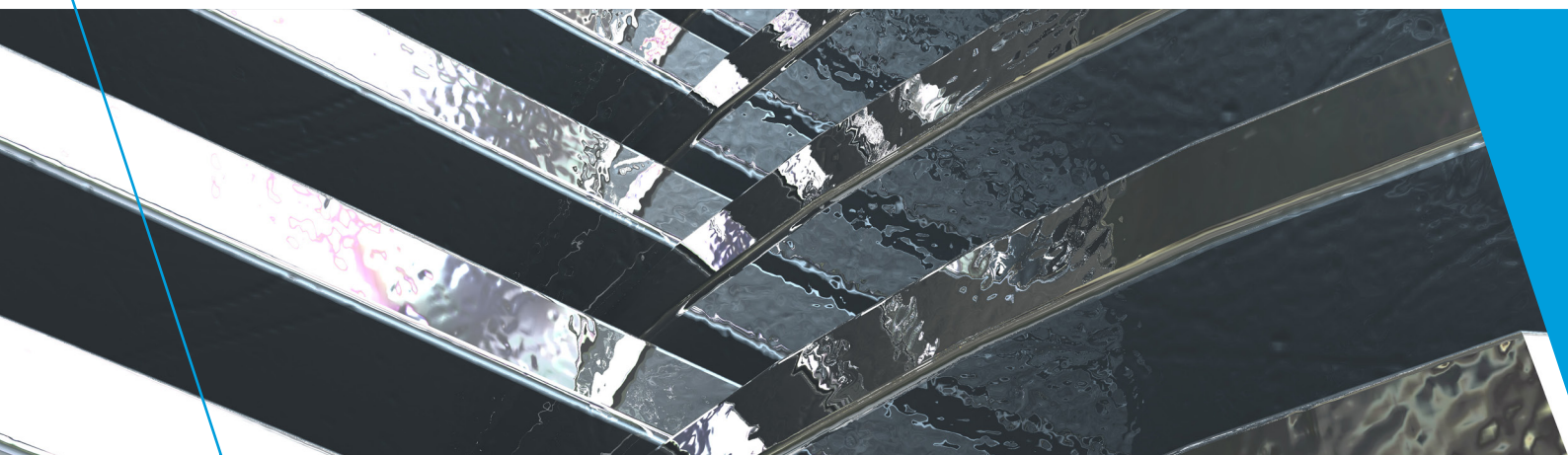
Australian Government

Australian Security Intelligence Organisation

T4 Protective Security

Protective security circular 167

Destruction of sensitive and security-classified information



www.asio.gov.au

Release history

Issue no.	Issue date	Description
1.0	2017	First release
2.0	2019	Change in NAID AAA Certified with PSPF endorsement transition date. Consolidate all destruction service advice into a single document.

Handling instructions

This document is protectively marked **OFFICIAL: Sensitive**, which means it contains information which if compromised may cause limited damage to national security, Australian Government agencies, commercial entities or members of the public.

You **must** take all reasonable action to protect and maintain the security of this document. This information should be shared only with individuals within your agency with a demonstrated 'need-to-know'.

This document **must** be stored in a lockable container and shredded before disposal. This document may be stored on electronic media but access **must** be limited to individuals within your agency with a demonstrated 'need-to-know'. Portable electronic media containing this document **must** be stored, handled and disposed of in accordance with the Australian Government *Protective Security Policy Framework* and *Information security manual*.

Disclaimer

The information provided in this document is intended to be used as general guidance material only and is not provided for any other purpose. In particular it is not intended to provide comprehensive advice on its subject matter or in relation to any particular product, and should not be relied upon as providing such advice. Organisations or individuals using or relying upon the information contained in this document are deemed to do so in conjunction with their own judgement and assessment of the information in light of their particular needs and circumstances. ASIO has taken every care in the preparation of this document to ensure the information is accurate at the time of publication. The Commonwealth, its officers, employees and agents exclude all liability for loss or damage (including in negligence) suffered or incurred by any organisation or individual as a result of their use of or reliance upon the information contained in this document.

© Commonwealth of Australia 2019

FOI STATEMENT

This document and any information, extract or summary from this document, is exempt under the *Freedom of Information Act 1982*. Refer related freedom of information requests to the Attorney-General's Department, Canberra.

Contents

Introduction	1
Purpose	1
Policy	1
Approved destruction methods	2
Approved destruction equipment	2
Destruction of paper-based sensitive and security-classified information	3
Paper shredding	3
Disintegrator and hammer mill	4
Microform pulverisation	4
Wet pulping	4
Incineration	4
Destruction of sensitive and security-classified information and information communications technology media	5
External destruction	5
Agency-approved destruction service	6
National Association for Information Destruction AAA Certification with PSPF endorsement destruction service	6
Inquiries and advice	7
Annex A: Criteria—agency-assessed destruction service	8
Annex B: Procedures guide	14
Introduction	14
Facility security	14
Personnel security	14
Collection	14
Transportation	14
Destruction	15
Incident reporting	15
Annex C: Searching the National Association for Information Destruction website	16

Introduction

Requirements for the external destruction of security-classified information have been updated due to changes in the Australian Government *Protective Security Policy Framework* (PSPF) and Australian Signals Directorate (ASD) *Information Security Manual* (ISM).

The Australian Security Intelligence Organisation T4 Protective Security Directorate (ASIO-T4) provides advice on the destruction of paper-based sensitive and security-classified information. ASD provides advice on the destruction of information and communications technology (ICT) media in the ISM.

ASIO-T4 no longer manages the ASIO-approved destruction service scheme. All companies on the ASIO-T4 Approved Destruction Services list have been extended until 30 June 2019. From 1 July 2019, all destruction companies wishing to destroy sensitive and classified information must meet National Association for Information Destruction (NAID) AAA Certification with PSPF endorsement or be an agency-approved destruction service as described in this protective security circular (PSC).

This PSC supersedes:

- ▶ ASIO-T4, *Criteria—agency-assessed and approved destruction service*;
- ▶ ASIO-T4, PSC 143—*Destruction of Australian Government Official Information*;
- ▶ ASIO-T4, PSC 144—*External destruction of Australian Government official information*; and
- ▶ ASIO-T4, PSC 167—*External destruction of Australian Government official information*.

Purpose

The purpose of this PSC is to advise Australian Government agencies of:

- ▶ the minimum requirements for the destruction of Australian Government sensitive and security-classified information;
- ▶ agency-approved destruction services; and
- ▶ external destruction service companies with NAID AAA Certification with PSPF endorsement.

Policy

The Australian Government's policy on the destruction of official information, including paper-based hardcopy material and ICT media, is detailed in:

- ▶ PSPF—*Sensitive and classified information*.
- ▶ ISM—*Guidelines for media management*

Approved destruction methods

Sensitive and security-classified information must be destroyed in accordance with the minimum requirements of the PSPF—*Sensitive and classified information, section C.3.6, and the ISM—Guidelines for media management*, using approved methods of destruction and approved destruction equipment.

Agencies should consider destroying security-classified information in-house using approved Class A and Class B shredders¹—minimising the risk of compromise during the collection, transportation and destruction of security-classified information.

Approved destruction equipment

Using approved destruction equipment can declassify sensitive and security-classified information down to an OFFICIAL level.

Approved destruction equipment includes:

- ▶ equipment listed in the Security Construction and Equipment Committee (SCEC) Security Equipment Catalogue and purchased before March 2015;
- ▶ equipment purchased after March 2015 and assessed by the agency against the relevant ASIO-T4 security equipment guides (SEG) listed below;
- ▶ equipment purchased after March 2015 and assessed by an independent test house, such as a National Association of Testing Authorities (NATA) test house, against the relevant ASIO-T4 test criteria; and
- ▶ equipment listed in the National Security Agency's evaluated products lists (and meeting the Australian Government particle size requirements).

Agencies should refer to the relevant ASIO-T4 SEG for guidance on testing and selecting equipment for the destruction of security-classified information.

- ▶ ASIO-T4, SEG-001 Class A and Class B paper shredders;
- ▶ ASIO-T4, SEG-009 Optical media shredders; and
- ▶ ASIO-T4, SEG-018 Destructors.

¹ Equipment listed in the Security Equipment Catalogue and purchased before March 2015.

Destruction of paper-based sensitive and security-classified information

	Shredding	Disintegrator and hammer mill	Microform pulverisation	Wet pulping	Furnace/ incinerator
TOP SECRET	Class A	3 mm mesh screen size	Fine powder	6 mm diameter aperture	Yes
SECRET	Class A	3 mm mesh screen size	Fine powder	6 mm diameter aperture	Yes
PROTECTED or protectively marked CABINET ²	Class B	9 mm mesh screen size	Fine powder	6 mm diameter aperture	Yes
OFFICIAL: Sensitive	Not applicable. Agency risk assessment. See paper-shredding section.	Not applicable. Agency risk assessment. See disintegrator and hammer mill section.	Not applicable. Agency risk assessment.	Not applicable. Agency risk assessment.	Not applicable. Agency risk assessment.
OFFICIAL	Not applicable.				

PSPF—*Sensitive and classified information, section C.3.6, states there are no security requirements imposed on the destruction of OFFICIAL: Sensitive information.* However, ASIO-T4 recommends the destruction of paper-based sensitive information is undertaken using a commercial cross-cut shredder. Agencies should not use commercial strip shredders for the destruction of paper-based sensitive information. If an agency decides to use commercial-grade equipment to destroy paper-based sensitive information, it should conduct an agency risk assessment to determine a suitable resultant particle size.

Paper shredding

Approved paper shredders must consistently shred paper without the resultant particles exceeding the maximum size allowed, or producing oversized or linked particles when operating at the maximum sheet capacity. Approved paper shredders must produce the following resultant particle size:

- ▶ **TOP SECRET** and **SECRET**—Class A (1 mm x 20 mm); and
- ▶ **PROTECTED**—Class B (2.3 mm x 25 mm).

ASIO-T4 recommends that paper-based **OFFICIAL: Sensitive** information:

- ▶ in low volumes is destroyed using Deutsches Instiut fur Normung (DIN) 32757.1 level 3³—3.9 mm x 30 mm
- ▶ in large volumes is destroyed using an external destruction service holding a NAID AAA Certification with PSPF endorsement for paper/printed media and ICT media protectively marked OFFICIAL: Sensitive.

² Information protectively marked CABINET must be destroyed using a minimum of PROTECTED requirements.

³ The majority of shredders sold in Australia are manufactured overseas, typically to meet the European standard Deutsches Instiut fur Normung (DIN) 32757.1.

Disintegrator and hammer mill

Disintegrators are suitable for destroying paper-based sensitive and security-classified information, and operate by means of an adjustable set of cylinder-mounted rotating cutting blades working in conjunction with a static cutter. The paper is ground down until the resultant particles are able to pass through a mesh screen, which is interchangeable to match the aperture size required for the security-classification of the information being destroyed. Hammer mills operate on a similar principle, except that hammer blades are used to shred or crush the paper.

- ▶ **TOP SECRET** and **SECRET**—use 3 mm mesh screen size; and
- ▶ **PROTECTED**—use 9 mm mesh screen size.

ASIO-T4 recommends paper-based **OFFICIAL: Sensitive** information:

- ▶ in low volumes is destroyed using 12 mm mesh screen size.
- ▶ in large volumes is destroyed using an external destruction service holding a NAID AAA Certification with PSPF endorsement for paper/printed media and ICT media protectively marked **OFFICIAL: Sensitive**.

Microform pulverisation⁴

Because microfilm and microfiche can contain very small characters, they need to be destroyed using a pulveriser that can reduce security-classified information to a fine powder.

The resultant particles must not show more than five consecutive characters per particle when subjected to microscopic inspection.

Microform should not be destroyed in disintegrators or hammer mills.

Wet pulping

Wet pulping is suitable for the destruction of paper-based sensitive and security-classified information. It operates by feeding paper into a pulping tank where it is mixed with water and drawn into a rotating cutter. The resultant slurry is then forced through a perforated sizing ring, and the excess water is extracted and returned to the pulping tank for reuse. The final product consists of a compacted, moist pulp which is approximately 20 per cent of the original volume.

A perforated particle sizing ring with a 6 mm diameter aperture is required for the destruction of paper-based security-classified information. A range of different aperture sizes is not generally provided with this type of equipment.

Incineration

Incinerators must reduce paper-based sensitive and security classified information to an ash powder. The resultant waste must not be capable of being reconstituted, and unburnt particles must not be able to escape via air vents or the stack. Incinerators must be inspected post-destruction to ensure there are no unburnt particles remaining.

Natural draft type

It is possible to add additional amounts of paper to a natural draft incinerator at almost any stage of the burning process. Consequently, this makes it possible to remove unburnt material from the incinerator or region of the incinerator at almost any time it is in use.

Pyrolytic type

It is not normally possible to open any part of the combustion chamber of a pyrolytic incinerator during the burning process without the risk of injury to the operator—material cannot be added to the incinerator once the burning cycle commences.

⁴ For the destruction of microform, only one machine is still available from the listed supplier in the SEC.

Destruction of sensitive and security-classified information and information communications technology media

To destroy ICT media—such as electrostatic memory devices, magnetic floppy discs, magnetic hard discs, magnetic tapes, optical discs and semi-conductor memory—agencies should break up, incinerate, or degauss the media. Agencies should refer to the destruction requirements for ICT media detailed in the ISM—*Guidelines for media management*. The following mesh screen sizes are required when using destruction methods to break up ICT media:

- ▶ **TOP SECRET**—3 mm mesh screen size;
- ▶ **SECRET**—3 mm mesh screen size;
- ▶ **PROTECTED**—9mm mesh screen size; and
- ▶ **OFFICIAL: Sensitive**—9mm mesh screen size.

ICT magnetic media may also be degaussed. Degaussing reduces the magnetisation of a magnetic storage device to zero by applying a reverse (coercive) magnetic force, rendering any previously stored information unreadable.

An agency must develop a procedure to identify if the ICT magnetic media has completed the degaussing process.

External destruction

Agencies may use an external destruction service company to destroy their sensitive and security-classified information.

Agencies have two options for external destruction:

- ▶ use an agency-approved destruction service; or
- ▶ use an external destruction service company with a NAID AAA Certification with PSPF endorsement.

All companies on the ASIO-T4 Approved Destruction Services list have been extended until 30 June 2019. From 1 July 2019, all destruction companies wishing to destroy sensitive and classified information must meet NAID AAA Certification with PSPF endorsement or be an agency-approved destruction service. If an external destruction service has not attained NAID AAA Certification with PSPF endorsement from the 1 July 2019, an agency must cease using the external destruction service company, or conduct an agency-approved destruction service assessment for agency-specific approval.

Before security-classified information is collected by a destruction service, the agency should consider how it will be stored in accordance with the PSPF; noting that, plastic 'secure document bins' used for storing security-classified information before collection are not SCEC-approved secure filing cabinets, nor do they meet the requirements of a lockable commercial grade cabinet. These bins must not be left unattended outside a security zone, such as in a building foyer or loading dock.

Agency-approved destruction service

Agencies may conduct their own assessment of an external destruction service company to destroy their sensitive or security-classified information.

They must use **Annex A**—‘Criteria—agency-assessed destruction service’ to assess destruction services for agency-specific approval.

An agency may apply additional security requirements to the **Annex A**—‘Criteria—agency-assessed destruction service’ requirements, such as providing security clearances for external destruction service company staff, or establishing appropriate security zones for handling and storing information before destruction.

Procedural control guidance is in **Annex B**—‘Procedures guide’.

National Association for Information Destruction AAA Certification with PSPF endorsement destruction service

NAID is the international trade association for companies providing information destruction services. The NAID AAA Certification program is a voluntary program for NAID members providing information destruction services. Third-party auditors engaged by NAID verify the qualifications of destruction service companies through two-yearly scheduled audits and random unannounced audits.

A company must hold NAID AAA Certification with PSPF endorsement for:

- ▶ paper/printed media and ICT media protectively marked OFFICIAL: Sensitive; and/or
- ▶ high security destruction for paper/printed media and ICT media for security classified information.

NAID AAA PSPF Certification does not include any process for the security clearance of destruction company staff. If an agency uses a NAID AAA service, collection, transportation and destruction of security classified information must be escorted and witnessed by trained and appropriately cleared agency staff (one staff member for SECRET and below, and two staff for TOP SECRET and codeword material). Alternatively, the agency may sponsor the clearance of destruction service staff involved in the collection, transportation and destruction of security-classified information.

Destruction must occur on the same-day of collection. If an Agency is wishing to destroy large volumes of information, they may need to be sequence their destruction to meet same-day destruction requirements. External destruction companies have no ability to store sensitive and security classified information as their premises is not rated to an equivalent security zone.

Should agencies have contractual obligations to continue using an existing ASIO-T4-approved destruction service beyond 30 June 2019, they should make the necessary arrangements to assess and approve the destruction service against the **Annex A**—‘Criteria—agency-assessed destruction service’, or encourage the service to seek NAID AAA Certification with PSPF endorsement.

See **Annex C**—‘Searching the NAID website’ for a list of external destruction service companies with NAID AAA Certification with PSPF endorsement.

Inquiries and advice

Agencies making inquiries or seeking advice on this PSC can contact ASIO-T4 by email at t4ps@t4.gov.au or by telephone on (02) 6234 1217.

Agencies can access the SEGs on *GovDEX*.

Annex A: Criteria—agency-assessed destruction service

Agencies must assess the destruction service against each part of the assessment criteria to confirm whether each measure has been implemented. Where measures have not been implemented, the agency should document the reason and any alternative measure(s) implemented to mitigate the risk of compromise during the collection, transportation and destruction of security-classified information.

In this criteria, the term **must** indicates mandatory minimum requirements.

The term **should** refers to requirements that are to be met unless there is a valid reason for an agency not to comply.

The term **recommend** refers to security best practice. Agencies are encouraged to document instances where they do not comply with security best practice.

Agency-assessed destruction service			
Pre-destruction		Implemented	
General		Yes	No
1.1	The agency should consider destroying security-classified information in-house using approved Class A shredders and Class B shredders.		
1.2	The agency must conduct a security risk assessment to ensure that the risks associated with the external destruction of security-classified information, including any foreign ownership risks, are managed appropriately.		
1.3	The agency should inspect the destruction service's transport, facility, equipment and procedures to confirm that the measures detailed in this criteria have been implemented.		
1.4	Before collection by a destruction service, the agency should consider how security-classified information will be stored in accordance with the PSPF; noting that, plastic 'secure document bins' used to store security-classified information before collection are not SCEC-approved secure filing cabinets, nor do they meet the requirements of a lockable commercial grade cabinet.		
1.5	The agency should ensure that staff involved in the external destruction process are made aware of the guidance detailed in this assessment criteria.		
1.6	The agency should ensure that companies undertaking work for the agency are aware of the requirements for the external destruction of security-classified information.		
1.7	The agency should ensure that companies contracted to provide property management services, such as arranging recycling and destruction services on behalf of the agency, are aware of the requirements for the external destruction of security-classified information.		
Contracts		Yes	No
2.1	It is recommended that a destruction service has operated as a commercial destruction service for a minimum of two years before being considered by an agency, to ensure it has a level of corporate knowledge about information destruction.		
2.2	The agency should ensure that tender documents and/or contract documents reflect Australian Government requirements for the destruction of security-classified information.		

2.3	The agency should require the destruction service to certify that it will collect, transport and destroy security-classified information in accordance with the PSPF, ISM and agency requirements.		
2.4	If the destruction service subcontracts the collection, transportation and/or destruction of security-classified information, the subcontractor must be agency-assessed or have NAID AAA Certification with PSPF endorsement for high security destruction for paper/printed media and ICT media for security classified information.		
2.5	The destruction service should be required to notify the agency in writing of significant changes to its circumstances, such as the site's physical address, physical security and construction, ownership, operations and approved equipment.		
2.6	The contract between the agency and the destruction service should address how non-compliance with Australian Government protective security requirements and breach of contract relating to protective security will be resolved.		
2.7	The destruction service should maintain records relevant to an agency assessment. It is recommended that the agency specifies a time frame for the records to be maintained.		
Collection, transportation and destruction		Yes	No
3.1	The agency should have an enclosed area where security-classified information can be loaded into the destruction service vehicle.		
3.2	The agency should ensure that the destruction service clearly labels secure document bins with the protective marking of the information permitted to be placed in the bins.		
3.3	The agency should ensure that secure document bins containing security-classified information are not left unattended during the collection process.		
3.4	The contents of secure document bins and/or classified waste bags must not be emptied into the rear of the vehicle and must not be transferred or tipped into other bins at the agency's premises.		
3.5	The agency should ensure the destruction service has the capacity to destroy the required volume of security-classified information before the close of business on the nominated day of destruction. This will mitigate the need to return security-classified information to the agency for secure storage.		
3.6	The transportation and destruction of security classified information must be escorted and witnessed by trained and appropriately cleared agency staff (one staff member for SECRET and below, and two staff for TOP SECRET and accountable). Alternatively, the agency may sponsor the clearance of destruction service staff involved in the collection, transportation and destruction of security-classified information.		
3.7	The destruction service should account for security-classified information (contained in document bins or classified waste bags) at three separate locations: ▶ loading; ▶ unloading; and ▶ feeding into destruction equipment.		

3.8	<p>The destruction service must have a set of operating procedures to support the destruction of security-classified information to ensure that staff involved in the collection, transportation and destruction process have clear instructions.</p> <p>Topics that should be covered in these procedures are listed at Annex B—‘Procedures outline’. The destruction service must maintain a register of staff who have been trained and have certified that they acknowledge and understand their obligations.</p>		
Vehicle security		Yes	No
4.1	Destruction service vehicles used to transport security-classified information must have a fully enclosed (with metal, fibreglass or other continuous panelling of equivalent strength) storage compartment to transport security-classified information. Compactor trucks and tautliner trucks must not be used.		
4.2	<p>Vehicles must be secured to prevent unauthorised access to security-classified information, including:</p> <ul style="list-style-type: none"> ▶ driver compartment should be secured, using factory locking, while in transit; ▶ driver compartment should be secured, using factory locking, while unattended; ▶ vehicles should not be left unattended for more than 15 minutes; and ▶ storage compartment locks should have fixed hinges and be secured with an SCEC-approved security level (SL) 3-rated padlock, or a padlock that meets the requirements of Australian Standards 4145.4:2002 <i>Locksets part 4: padlocks lock</i>, with a minimum Padlocks Physical Security (SP) rating 6, and fitted with an SCEC-approved keying system. See SEG 28—<i>Padlocks</i> for more guidance. 		
4.3	Destruction services must collect security-classified information from the agency on dedicated trips, to reduce the risk of information being compromised at other collection points and to decrease the time frame between collection and destruction.		
4.4	Destruction services must allow agency staff to escort the vehicle.		
Facility security		Yes	No
5.1	The destruction service facility must have an enclosed area to unload security-classified information to reduce the risk of information being compromised during unloading.		
5.2	The destruction service facility must have physical security measures (for example, fences, walls, doors, access control) to mitigate the risk of unauthorised individuals accessing the facility during the destruction of security-classified information.		
5.3	The destruction service must implement visitor management processes (including escorting) to mitigate the risk of visitors compromising security-classified information during unloading and destruction.		
5.4	<p>The destruction service must have a discrete area within the facility where security-classified information is destroyed, to mitigate the risk of unauthorised individuals accessing the area during the destruction of security-classified information, including:</p> <ul style="list-style-type: none"> ▶ an enclosed area with its perimeter forming part of the existing building fabric or chain link fence at least 1.8 m high; and ▶ a gate or door that can be locked from the unsecure side (that is, requires a key to enter) and enables egress from the secure side (for example, a turn snib). 		

5.5	Unless the agency (or ASIO-T4 for Zone 5 areas) has certified and accredited the destruction service facility for the storage of security-classified information, security-classified information must not be stored in the facility overnight. Procedures must be in place to return security-classified information to the agency if it cannot be destroyed before the close of business.		
Destruction		Yes	No
6.1	The destruction service must destroy security-classified information using an approved method in accordance with PSC 167 and ISM.		
6.2	<p>Destruction services must have approved equipment installed to enable the destruction of security-classified information to the required particle size for the classification of the information. Approved destruction equipment includes:</p> <ul style="list-style-type: none"> ▶ equipment listed in the ASIO-T4 Security Equipment Catalogue and purchased before March 2015; ▶ equipment purchased after March 2015 and assessed by the agency against the relevant ASIO-T4 SEG; ▶ equipment purchased after March 2015 and assessed by an independent test house, such as a National Association of Testing Authorities (NATA) test house, against the relevant ASIO-T4 test criteria; ▶ equipment listed in the National Security Agency's evaluated products lists (and meeting the Australian Government particle size requirements). 		
6.3	Agencies should ensure that the approved equipment of destruction services is assessed every five years from March 2015 or from the date of purchase (if purchased after March 2015) by an independent test house, such as a NATA test house, against the relevant ASIO-T4 test criteria.		
6.4	The destruction of security-classified information should be performed immediately after the information has arrived at the destruction facility.		
6.5	The destruction service must have screen sizes that meet the required particle size for the classification of the information being destroyed.		
6.6	Destruction services must allow agency staff to physically confirm the correct screen is installed; witness the destruction; and inspect conveyor belts, feed chutes and cutting chambers after the destruction process is completed, to ensure all security-classified information has been destroyed to the particle size requirements for the classification.		
6.7	<p>At the initial assessment inspection, agencies should collect a sample of each type of media to take away for testing.</p> <p>It is recommended that the agency processes each type of media separately in a laboratory test sieve with an aperture size no greater than the smallest screen size (plus 5 per cent tolerance) the destruction service is seeking to use. For example, if the destruction service is seeking to use a 3 mm screen, the aperture size in the sieve should be no greater than 3.15 mm.</p> <p>The agency should use the test sieve to verify that the resultant particles are consistent with the smallest screen size the destruction service is seeking to use.</p>		
6.8	Where required by the PSPF and the agency, the destruction service must provide a destruction certificate.		

Personnel security		Yes	No
7.1	<p>The destruction service must conduct the following personnel checks before engaging an individual to collect, transport and destroy security-classified information:</p> <ul style="list-style-type: none"> ▶ identity checked to level 2 of the National Identity Proofing Guidelines upon engagement; ▶ national police history check conducted by a National Police Checking Service–accredited organisation or police (before engagement and every three years thereafter); ▶ current driver's licence confirmed before engagement and every six months thereafter; and ▶ visa check conducted for staff who are not Australian citizens or permanent residents, to ensure they hold a current work visa, and ensure that those staff continue to hold current work visas for the duration of their employment or engagement with the destruction service. <p>The destruction service must maintain a register of personnel checks. It is recommended that the agency specifies a time frame for the register to be kept.</p>		
7.2	<p>The destruction service must require staff (and subcontractors) to identify themselves when collecting security-classified information:</p> <ul style="list-style-type: none"> ▶ All staff should carry photographic identification (ID). ▶ The ID should display the company logo. ▶ The ID should detail the full name or an identification number of the staff. ▶ The ID should detail a clearly visible issue and expiration date. 		
7.3	The destruction service should require destruction service staff to wear a company uniform.		
7.4	The agency should ensure that destruction service staff involved in the collection, transportation and destruction of security-classified information sign confidentiality and non-disclosure agreements.		
7.5	The destruction service must provide annual security awareness briefings and operational training for the collection, transportation and destruction of security classified information.		
7.6	Destruction service staff should annually sign an acknowledgement that they have attended security awareness training and operational training and have read and understood their obligations in regard to the collection, transportation and destruction of security-classified information.		
Contingency		Yes	No
8.1	A destruction service must develop and implement contingency plans to take effect when security incidents occur. These include transportation issues and equipment breakdowns which affect the timely collection, transportation and destruction of security-classified information.		
During destruction		Yes	No
9.1	The destruction service should ensure the discrete area is clear of other waste material, to help agency staff inspect the area before and after the destruction of security-classified information.		
9.2	Agency staff should sight that the correct screen size for the classification of the information being destroyed is installed in the destruction equipment.		
9.3	Agency staff should ensure security-classified information is not removed from the destruction equipment before the destruction process is complete.		
9.4	It is recommended that agency staff confirm with the destruction service that the cutting blades are well maintained and changed periodically to ensure good throughput. Depending on the type and volume of security-classified information being destroyed, the cutting blades can become blunt, which can slow throughput.		

After destruction		Yes	No
10.1	Agency staff should inspect conveyor belts, feed chutes and cutting chambers to ensure all security-classified information has been destroyed to the particle size required for the classification of the information. If oversized particles are found in the destroyed waste: <ul style="list-style-type: none"> ▶ the screen may be damaged; ▶ the seal between the screen and the cutting chamber may not be intact; or ▶ material may be left over from a previous production run using a larger screen size. 		
Ongoing performance		Yes	No
11.1	Agencies should implement measures for the ongoing performance monitoring of the destruction service.		
11.2	Agencies should consider re-inspecting the destruction service periodically to ensure that PSPF and agency contract requirements are being met.		
Reporting		Yes	No
12.1	A destruction service must notify the agency when a security incident involving the collection, transportation or destruction of security classified information occurs. The time frame for a destruction service to report an incident should be determined by the agency.		
12.2	The agency must report security incidents involving the compromise of security-classified information in accordance with the PSPF and ISM.		
Advertising		Yes	No
13.1	The destruction service should not make reference to Australian Government agency approvals or endorsements for the collection, transportation and destruction of Australian Government official information or security-classified information in the facilities, on vehicles, in web pages, emails, business cards, yellow page entries and/or in other media advertising. This measure provides a level of anonymity for security-classified information and helps make it indistinguishable from the destruction service's standard commercial service.		

Annex B: Procedures guide

A destruction service **must** have a set of operating procedures to support the destruction of security-classified information and to ensure that staff involved in the collection, transportation and destruction process have clear instructions.

Topics that should be covered in these procedures are listed below.

Introduction

- ▶ general company information
- ▶ purpose of procedures
- ▶ relevant Australian Government policy
- ▶ Australian Government protective markings
- ▶ roles and responsibilities of management and staff

Facility security

- ▶ physical security measures
- ▶ visitor management and escorting
- ▶ access control into the facility and discrete area

Personnel security

- ▶ identification check, national police checks, visa checks and licence checks
- ▶ identification cards
- ▶ security briefings and training
- ▶ confidentiality briefings

Collection

- ▶ collection and loading procedures
- ▶ security of document bins and classified waste bags
- ▶ security of vehicles during collection
- ▶ counting and accounting for material

Transportation

- ▶ type of vehicles used
- ▶ security of vehicle during transit
- ▶ dedicated runs
- ▶ unloading procedures
- ▶ counting and accounting of material
- ▶ agency escort

Destruction

- ▶ description of destruction equipment
- ▶ required screen sizes for paper-based information and ICT media
- ▶ destruction procedures
- ▶ counting and accounting of material
- ▶ agency witness
- ▶ contingency plans
- ▶ destruction certificates

Incident reporting

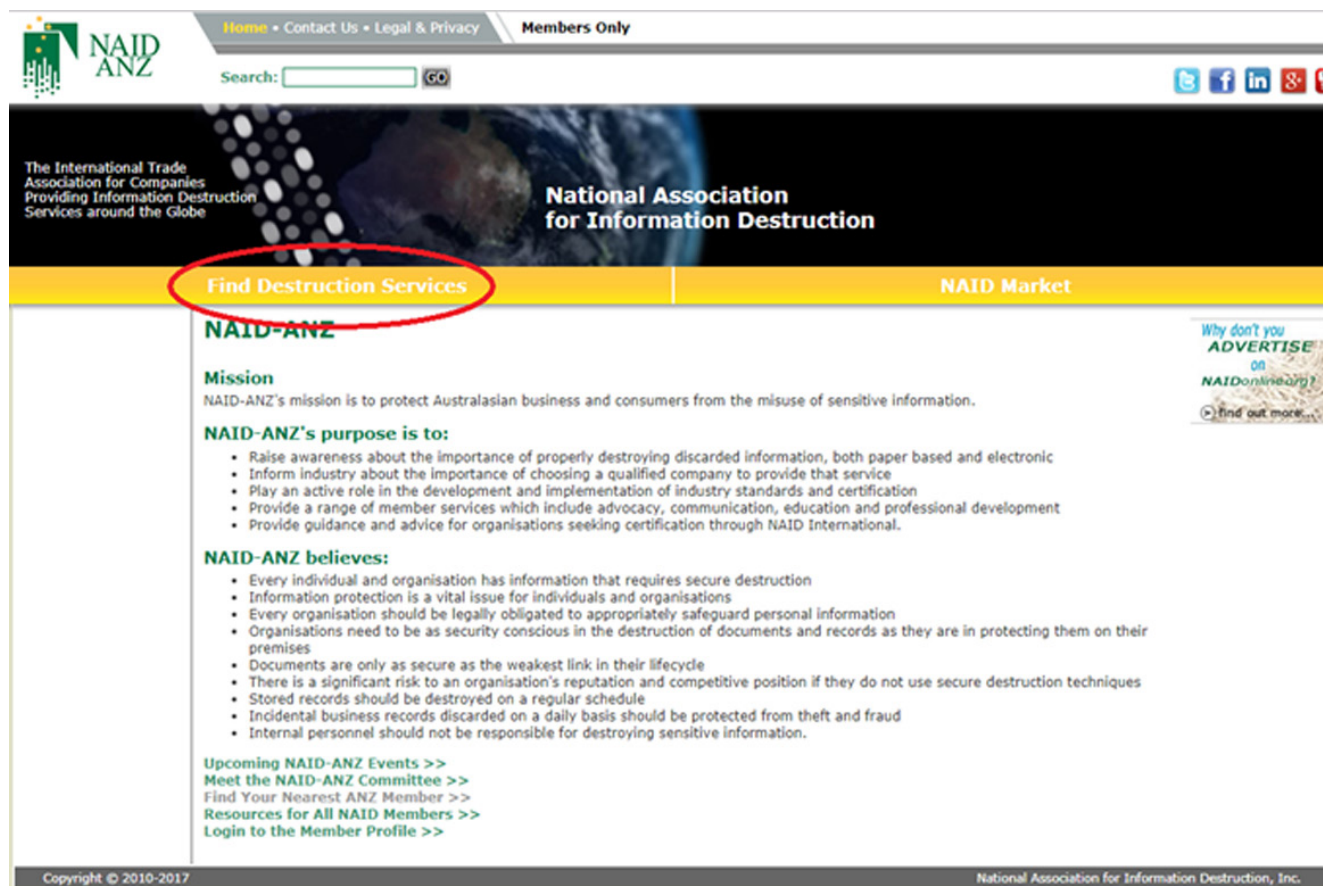
- ▶ reporting requirements

Annex C: Searching the National Association for Information Destruction website

Destruction services which are NAID AAA Certified with PSPF endorsement can be found at www.naidonline.org/naus/en/index.html

Instructions on how to find a destruction service with NAID AAA Certification are detailed below.

1. Go to the NAID website front page and select Find Destruction Services.



The screenshot shows the NAID-ANZ website. At the top, there is a navigation bar with links: Home, Contact Us, Legal & Privacy, and Members Only. Below this is a search bar with the text "Search:" and a "GO" button. The main header features the NAID-ANZ logo and the text "The International Trade Association for Companies Providing Information Destruction Services around the Globe" and "National Association for Information Destruction". A yellow navigation bar contains two links: "Find Destruction Services" (which is circled in red) and "NAID Market". Below the navigation bar, the "NAID-ANZ" section is visible, containing a "Mission" statement, "NAID-ANZ's purpose is to:" followed by a list of bullet points, "NAID-ANZ believes:" followed by a list of bullet points, and a list of "Upcoming NAID-ANZ Events" with links to "Meet the NAID-ANZ Committee", "Find Your Nearest ANZ Member", "Resources for All NAID Members", and "Login to the Member Profile". A small advertisement on the right side asks "Why don't you ADVERTISE on NAIDonline.org?". The footer contains the copyright notice "Copyright © 2010-2017" and the text "National Association for Information Destruction, Inc."

2. Search for a service company – NAID AAA Certified Members and Australian PSPF Endorsed.

Search by Name or Location (optional)

Company Name:
(Find a specific company by name)

or Location Focus:
(Enter Zip Code, City & State, Province, or Country as a search area focus)

50km from center ▾

Filter by: ?

☐ All I-SIGMA Members
☐ All NAID Members
☒ NAID AAA Certified Members
☐ All PRISM International Members
☐ All Privacy+ Members

Exclusive Offerings ?

☐ Licensed to provide NAID Customer Employee Training
☐ Indemnified by Downstream Data Coverage

Select "NAID AAA Certified Members" as a filter above to activate these options

NAID AAA Certified for:

Service Platform ?

☐ Plant-Based
☐ Mobile/On-site

Data Destruction Services ?

☐ Paper Records Destruction
☐ Micro-Media Destruction
☐ Non-paper Media Destruction
☐ Computer Media Destruction-Physical
☐ Computer Media Destruction-Sanitization
☐ Degaussing Operations
☐ Product Destruction

NEW Australian PSPF Endorsed ?

☒ Australian operations endorsed for destruction of Official Information under the country's Protective Security Policy Framework (PSPF)

Custodial Operations ?

☐ Data Recovery/Forensic and Breach Investigation
☐ Online Backup

Step 2: View Results

8 Results Found

[Clear Selections](#)

3. Click on a certified service company in the desired location. Details such as contact details, endorsements, approved equipment, type of media the equipment is approved to destroy, screen size, and certification expiry date will be displayed.

Address Info	NAID Certified Services
Contact Name: AAA Destruction Service Address: 4 Shredder Road City: Canberra State: ACT Country: Australia Phone: 02 6000 000 Fax: Email: aaadestructionservice@internet.com.au Website: www.aaadestructionservice.com.au	<ul style="list-style-type: none"> Plant-based paper records destruction (same day destruction) Plant-based High security destruction <ul style="list-style-type: none"> + Disintegrator <ul style="list-style-type: none"> - Paper, optical media, magnetic tape - 3 mm, 6 mm and 9 mm screens + Hammer Mill <ul style="list-style-type: none"> - optical media and hard drives - 3 mm and 9 mm screens <p>Originally Certified: 10/18/2013 Certification Expires: 5/27/2017</p>

4. Use the displayed details to confirm that the service company has the required mesh screen sizes to destroy security-classified information to the particle size required for the security classification of the information.

