Information security management guidelines

Protectively marking and handling sensitive and security classified information

Approved June 2011

Amended May 2018

Version 1.4
© Commonwealth of Australia 2016

All material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

[CC BY]

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It’s an Honour website (www.itsanhonour.gov.au).

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Attorney-General’s Department
3–5 National Cct
BARTON ACT 2600

Email: copyright@ag.gov.au

<table>
<thead>
<tr>
<th>Document details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security classification</td>
<td>Unclassified</td>
</tr>
<tr>
<td>Dissemination limiting marking</td>
<td>None</td>
</tr>
<tr>
<td>Date of security classification review</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Authority</td>
<td>Protective Security Policy Committee</td>
</tr>
<tr>
<td>Author</td>
<td>Attorney-General’s Department</td>
</tr>
<tr>
<td>Document status</td>
<td>Approved 21 June 2011</td>
</tr>
<tr>
<td></td>
<td>Amended June 2015</td>
</tr>
<tr>
<td></td>
<td>Amended November 2017</td>
</tr>
</tbody>
</table>
Part 2 Procedures for protecting protectively marked documents and material ......................... 17

4. Procedures for control of protectively marked information .................................................. 18
   4.1 Registration systems ........................................................................................................... 18
   4.2 Audit .................................................................................................................................... 18
   4.3 Spot checks .......................................................................................................................... 18
   4.4 Physical files holding protectively marked information .................................................... 19
   4.5 Storage of sensitive and security classified information ..................................................... 20
   4.6 Aggregation of protectively marked information ............................................................... 20

5. Procedures for production and reproduction of protectively marked documents ................... 22
   5.1 General ............................................................................................................................... 22
   5.2 Accountable Material ........................................................................................................ 22
   5.3 Foreign government information (FGI) ............................................................................. 22
   5.4 Photocopiers, facsimile machines and similar devices ....................................................... 22

6. Removal of protectively marked documents and material from agency premises .................. 24
   6.1 General ............................................................................................................................... 24
   6.2 Within Australia .................................................................................................................. 24
   6.3 Outside Australia ................................................................................................................ 25

7. Procedures for the transfer of protectively marked information and material ....................... 26
   7.1 General ............................................................................................................................... 26
   7.2 Preparing protectively marked information for physical transfer ..................................... 26
   7.3 Process for double enveloping .......................................................................................... 27
      7.3.1 Outer envelope .............................................................................................................. 27
      7.3.2 Inner envelope .............................................................................................................. 28
      7.3.3 Other methods .............................................................................................................. 28

8. Methods of transfer ............................................................................................................. 29
   8.1 Safe hand ............................................................................................................................ 29
   8.2 Carriage by SCEC-endorsed commercial courier .............................................................. 29
   8.3 Bulky material .................................................................................................................... 30
8.4 High risk unclassified material

9. Receiving protectively marked documents
   9.1 General
   9.2 Foreign government information

10. Procedures for the destruction of protectively marked documents and ICT media
    10.1 General
    10.2 Methods of destruction
    10.3 Garbage and recycling
    10.4 External destruction
    10.5 ICT media and equipment
    10.6 Microfiche and other photographic material

Table: Control and handling of security classified documents and material
## Amendments

<table>
<thead>
<tr>
<th>No.</th>
<th>Date</th>
<th>Location</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>May 2012</td>
<td>Section 3.7</td>
<td>Update country codes to ISO 3166-01 Alpha 3 codes.</td>
</tr>
<tr>
<td>2</td>
<td>April 2015</td>
<td>Summary Table all levels – physical transfer</td>
<td>Delete – delivered by an agency specific alternative approved by ASIO.</td>
</tr>
<tr>
<td>3</td>
<td>April 2015</td>
<td>Throughout</td>
<td>Update links.</td>
</tr>
<tr>
<td>4</td>
<td>April 2015</td>
<td>Throughout</td>
<td>Number paragraphs.</td>
</tr>
<tr>
<td>6</td>
<td>April 2015</td>
<td>Paragraph 126</td>
<td>Replace SEC with Security equipment evaluated product list.</td>
</tr>
<tr>
<td>7</td>
<td>April 2015</td>
<td>Paragraph 158</td>
<td>Include reference to SEG 143 for selecting destruction equipment.</td>
</tr>
<tr>
<td>8</td>
<td>April 2015</td>
<td>Paragraph 171</td>
<td>Replace SEC with reference to SEG 143.</td>
</tr>
<tr>
<td>9</td>
<td>May 2015</td>
<td>Paragraph 4</td>
<td>Replace ‘physical information security core policy’ with ‘information security core policy’.</td>
</tr>
<tr>
<td>10</td>
<td>May 2015</td>
<td>Paragraph 17</td>
<td>Include reference to caveats as a protective marking</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Include left hand margin position for paragraph grading indicators.</td>
</tr>
<tr>
<td>11</td>
<td>May 2015</td>
<td>Paragraph 20</td>
<td>Add paragraph on document classification</td>
</tr>
<tr>
<td>12</td>
<td>May 2015</td>
<td>Table</td>
<td>Include end of paragraph position for paragraph grading indicators.</td>
</tr>
<tr>
<td>13</td>
<td>June 2015</td>
<td>Table</td>
<td>Remove inconsistency in wording for transfer of information within Australia</td>
</tr>
<tr>
<td>14</td>
<td>November 2017</td>
<td>Section 10</td>
<td>Update procedures for the destruction of protectively marked documents and ICT media</td>
</tr>
<tr>
<td>15</td>
<td>May 2018</td>
<td>Section 6.3 Paragraph 103</td>
<td>Updated weight limit on safehand bags as advised by DFAT</td>
</tr>
</tbody>
</table>
1. Introduction

1.1 Purpose
1. The Australian Government information security management guidelines—Protectively marking and handling sensitive and security classified information and material provides guidance on the protective marking and handling of sensitive and security classified information. This includes security classified information, information bearing dissemination limiting markers (DLM) and applying caveats.

1.2 Audience
2. This document is primarily intended for Australian Government employees, those contracted to the Australian Government and other individuals who require access to this information. See Protective Security Policy Framework (PSPF).

1.3 Scope
3. These guidelines relate to information security within the Australian Government.

1.3.1 Use of specific terms in these guidelines
4. In these guidelines the terms:
   - ‘need to’—refers to a legislative requirement that agencies must meet
   - ‘are required to’ or ‘is required to’—refer to a control:
     - to which agencies cannot give a policy exception, or
     - used in other protective security documents that set controls
   - ‘are to’ or ‘is to’—are directions required to support compliance with the mandatory requirements of the information security core policy, and
   - ‘should’—refers to better practice; agencies are expected to apply better practice unless there is a reason based on their risk assessment to apply alternative controls.

5. For details on policy exceptions see the Australian Government information security management protocol.
2. Background

2.1 Why these guidelines were developed
6. These guidelines aim to provide a consistent and structured approach to protectively marking and handling Australian Government sensitive and security classified information and material.

2.2 Relationship to other documents
7. These guidelines support the implementation of the PSPF. In particular it supports the Australian Government information security core policy.

8. It is part of a suite of documents that assist agencies to meet their information security mandatory requirements. It should be read in conjunction with the Australian Government information security management protocol and other supporting guidelines.

2.3 How these guidelines are structured
9. These guidelines introduce the application of protective markings and go on to describe handling procedures for sensitive and security classified information and material including:

- removal of protectively marked information and material from agency premises
- transfer of protectively marked information and material
- receipt of protectively marked hardcopy information and material, and
- destruction of protectively marked hardcopy information and material.
Part 1

Marking sensitive and security classified documents and material
3. **Procedures for applying protective markings**

10. Official information requiring protection is to be made visually different by the use of protective markings. This is relatively easy in the case of information held as a document either on paper or electronically. The following describes procedures for applying protective markings.

11. It is recommended that agencies protectively mark each paragraph within a document that requires a security classification. Agencies should develop their own policy on the application of DLMs for paragraphs marking. The overall classification of the document will, as a minimum, be equal to the highest classification level of any one paragraph in the document.

12. For guidance on how to identify whether information requires protective markings, agencies are to follow the *Australian Government information security management guidelines—Australian Government security classification system*.

13. For guidance on how to protectively mark foreign government information, agencies are to follow the *Australian Government protective security governance guidelines—Safeguarding foreign government information*.

14. The originator is to conspicuously mark all documents requiring protection with the appropriate protective marking. It is preferred that agencies place protective markings at the top and bottom of each page where possible. A document in this context is any form of recorded information such as reports, letters, books, e-mail, minutes, memoranda, films, charts, tapes, images and digital media.

15. If sensitive or security classified information is delivered orally, as through classified discussions, the recipient should be told if it requires protections.

16. Documents with covers, such as books, pamphlets and reports, are to show the protective marking on the front cover, title page, rear cover and, if possible, on the binding in addition to each individual page. Any binding or fastening of pages cannot obscure the protective marking.
3.1 Applying paragraph grading indicators

17. Protective markings, including caveats, on paragraphs are known as paragraph grading indicators and may appear in a consistent position:
   
   - in brackets at the end of each paragraph
   
   or
   
   - in the left margin, adjacent to the first letter of the paragraph.

18. The protective marking can be written in full or abbreviated by the first letters of the markings and should be the same colour as the text within the document. For instance, (S) for SECRET or (P) for PROTECTED.

19. Agencies, when applying paragraph grading indicators, should consider using the marking (U) for UNCLASSIFIED for paragraphs that do not carry a protective marking.

20. Agencies are to ensure that the protective marking of the whole document should be equal to the highest protectively marked paragraph.

Example 1: Applying paragraph grading indicators

---

**SECRET**

Subject: Examples (U)

1. Paragraph 1 contains ‘UNCLASSIFIED’ information and may be marked with ‘U’ in brackets at the end of the paragraph.

   (U)

   - If all sub-paragraphs are the same classification as the primary paragraph, then you do not need to mark the sub-paragraphs.
   
   - However, if the portions are not all the same classification, then all main and sub-paragraphs may be individually marked. (S)

**OR**

(U) Subject: Examples

(U) 1. Paragraph 1 contains ‘UNCLASSIFIED’ information and may be marked with ‘U’ in brackets in the margin to the left of the paragraph.

   • If all sub-paragraphs are the same classification as the primary paragraph, then you do not need to mark the sub-paragraphs.
   
   • However, if the portions are not all the same classification, then all main and sub-paragraphs may be individually marked.

**SECRET**

---

In this example SECRET is the security classification of this paragraph, which is indicated by using (S) at the end of the paragraph.
3.2 Applying an overall protective marking

21. Once the paragraph grading indicators have been applied, the overall protective marking can be established. This will be, as a minimum, equal to the highest classification level of any one paragraph within the document.

22. Security classifications and caveats are to be in capitals, bold text and a minimum of 5 mm high (preferably red) – for example, CONFIDENTIAL or TOP SECRET. DLMs are marked using capitals for each word, in bold text and a minimum of 5 mm high (preferably red)—for example, For Official Use Only or Sensitive.

23. Conspicuously place the overall security classification at the top and bottom of each page. The header can be stacked to fit around the letterhead, otherwise a single line is suitable. If an agency’s computer system can generate printed protective markings in red, which is preferable. If an existing document requires its protective marking to be applied using a stamp, the stamp should be in red.

24. Where a document requires both a security classification and a DLM, the security classification is applied to the top and bottom of the page. The DLM is placed below the top security classification and above the bottom of the security classification. See Example 5: Applying a security classification and DLM to the same document.

25. The DLM ‘Sensitive’ can be used alone or in conjunction with a document security classification where there is security classified information as well as information that warrants the ‘Sensitive’ marking.

26. When agencies apply a DLM of ‘Sensitive’ they are to include a footer on the first page, or a separate cover page, that identifies the reason for the ‘Sensitive’ marking and the handling requirements for the document as a result of the marking.

Example 2: Front page

Sensitive

The attached document contains Sensitive information

Reason for marking, e.g. This document may contain protected information as defined under the Social Security Act 1991

Sensitive

Cover sheet

Reason for marking, e.g. This document may contain protected information as defined under the Social Security Act 1991

This document is to be handled......>

27. When agencies use a DLM of ‘Sensitive’ in conjunction with a security classification and the handling requirement for the security classification is more stringent that any handling requirements arising from the DLM, then there is no need to include a handling requirement. For example, PROTECTED Sensitive: Cabinet is handled as PROTECTED information. The reason for the ‘Sensitive’ DLM is still required.
Example 3: Applying a security classification

21 April 2011
Mr John Smith
Chief Executive Officer
Department of Classified Documents
CANBERRA CITY ACT 2601

Subject: Examples

1. Paragraph 1 contains UNCLASSIFIED information. This portion may be marked with 'U' in brackets at the end of the paragraph. (U)

2. Paragraph 2 contains CONFIDENTIAL information. This portion may be marked with 'C' in brackets at the end of the paragraph. (C)

3. Paragraph 3 contains PROTECTED information. This portion may be marked with 'P' in brackets at the end of the paragraph. (P)

In this example (C) is the highest classification in this document, therefore CONFIDENTIAL is the overall classification.
Example 4: Applying a DLM

For Official Use Only

21 April 2011
Mr John Smith
Chief Executive Officer
Department of Classified Documents
CANBERRA CITY ACT 2601

Subject: Examples

1. Paragraph 1 contains UNCLASSIFIED information. (U)

2. Paragraph 2 contains ‘For Official Use Only’ information. (FOUO)

3. Paragraph 3 contains UNCLASSIFIED information. (U)

In this example, ‘For Official Use Only’ is the overall DLM.
Example 5: Applying a security classification and DLM to the same document

In this example the security classification PROTECTED is applied to the top of the page with the DLM ‘Sensitive: Legal’ placed below the security classification.

In this example (P) is the highest classification in this document, therefore PROTECTED is the overall classification.

In this example the security classification PROTECTED is applied to the bottom of the page with the DLM ‘Sensitive: Legal’ placed above the security classification.

21 April 2011
Mr John Smith
Chief Executive Officer
Department of Classified Documents
CANBERRA CITY ACT 2601

Subject: Examples

1. Paragraph 1 contains ‘For Official Use Only’ information. Therefore, this portion may be marked FOUO in brackets at the end of the paragraph. (FOUO)

2. Paragraph 2 contains ‘Sensitive: Legal’ information. (Sens: L)

3. Paragraph 3 contains PROTECTED information. This portion may be marked with ‘P’ in brackets at the end of the section. (P)
Example 6: Applying a protective marker to a multiple page document.

In this example the document contains more than one page, therefore the overall marking is placed at the top and bottom of the outside of the front cover, title page, on all pages in the document, and on the outside of the back cover.
3.3 Protectively marking titles

28. Wherever possible the titles of files, documents, books, reports, etc should not be protectively marked.

29. If protectively marking the title is essential, the originator should use a separate UNCLASSIFIED reference. This can appear behind the title in brackets.

30. Protectively marked classified titles are not to appear in information, documents or records management systems that are not themselves protectively marked.

3.4 Printed graphic matter

31. The protective markings for maps, drawings, etc, are to be printed or stamped near the map scale or drawing numbers as well as printed at the top and bottom centre of the document.

32. If the sheet is to be folded, the marking is to remain visible after folding.

3.5 Protectively marking annexes, appendixes, attachments and covering documents

33. In some cases the annexes or appendixes to a document will require protective markings even if the rest of the document can remain unclassified. Sometimes the annex or appendix requires a different protective marking from the document itself.

34. If the annex, appendix or attachment has a higher security classification than the principal document, the document’s front cover is to indicate that the document as a whole covers a higher security classification. This is not required where the annex, appendix or attachment is of a lower security classification.

35. When security classified paper-based documents are filed, the file security classification should be clearly visible. The same is true for removable electronic and optical media, such as USB, CD-ROMs, microfilms, photographs and removable hard drives. Refer to the Australian Signals Directorate’s (DSD) Australian Government Information Security Manual (ISM) section on media security.
Example 7: Applying security classifications to annexes and appendixes

In this example the header is stacked to fit around the letterhead etc. Otherwise a single line is preferred.

In this example the appendix has a higher classification than the principle document; therefore the front cover indicates that the document as a whole covers a higher classification.

In this example (TS) is the appendix to the principle document.
3.6 Caveats

36. Agencies are to refer to the *Australian Government information security management guidelines—Australian Government security classification system* for guidance on caveats.

37. Example 8 shows how to apply a caveat marking to a document.

**Example 8: Applying caveats**
3.7 ‘RELEASABLE TO’ and special handling caveats

38. Agencies are to refer to the Australian Government information security management guidelines—Australian Government security classification system for guidance on ‘RELEASABLE TO’ and special handling caveats. ‘RELEASABLE TO’ markings are to employ the appropriate three letter country codes from ISO 3166-1 Codes for the representation of names of countries and their subdivisions—Part 1: Country codes.

39. ‘RELEASABLE TO’ is to appear in capital letters.

40. Example 9 shows how to apply ‘RELEASABLE TO’ and special handling caveats to a document.

Example 9: Marking ‘RELEASABLE TO’ and special handling caveats

---

SECRET RELEASABLE TO GBR, NZL

PROTECTED
EXCLUSIVE FOR (named person)

SECRET RELEASABLE TO GBR, NZL

EXCLUSIVE FOR (named person)
PROTECTED
3.8 Protectively marking Cabinet documents

41. All documents prepared for considerations by Cabinet, including those in preparation are, as a minimum, to be protectively marked ‘Sensitive: Cabinet’ and carry the security classification PROTECTED, regardless of any other security consideration. See Example 10.

42. Cabinet documents can require a higher level of protection, depending on whether their subject matter is considered a national security issue. In this case the Cabinet document is to show, immediately before the DLM ‘Sensitive: Cabinet’, one of the higher protective markings. See Example 10.

Example 10: Applying a protective marker and security classifying Cabinet documents

PROTECTED
Sensitive: Cabinet

SECRET
Sensitive: Cabinet
3.9 Imagery

43. Sensitive and security classified photographs and film and their storage envelopes or containers are to carry a conspicuous protective marking.

44. As well as having the protective marking on both sides of the containers and spools, sensitive or security classified imagery—including roll imagery, cine-film, video tape—requires a protective marking in the title and end sequences to ensure projection of the marking for at least five seconds for each.

45. Agencies should mark photographic negatives so that the protective marking is reproduced on all copies made from that negative.

3.10 Presentations

46. Agencies are to apply appropriate protective markings to sensitive and security classified presentations. Each slide or screen is to be treated as an individual page, as in a paper-based document.

3.11 Audio

47. For audio recordings, the level of protective marking is to be clearly stated at the beginning and end of each recording. The tape or other media and its container are to be conspicuously labelled with the appropriate protective marking.

3.12 Microforms

48. Agencies may still hold microforms such as aperture cards, microfiche and microfilm containing sensitive and security classified information. If so, this material is to show the appropriate protective marking at the top and bottom centre of each frame. Additionally, containers and envelopes are to bear the appropriate protective marking of the highest protectively marked microform.

49. The protective marking is to be visible without projection on both cards and fiche, and microfilm is to be prominently marked at the beginning and end of each roll.

3.13 Electronic storage media

50. Policy for the marking of electronic storage media is contained in the ISM under Media Security.

3.14 Equipment

51. Agencies are to develop specific procedures for the placement of protective markings on equipment. This protective marking should be clearly visible and not easily removed.
Part 2

Procedures for protecting protectively marked documents and material
4. Procedures for control of protectively marked information

4.1 Registration systems

52. Agencies are to have in place a system for the control and handling of sensitive and security classified information in accordance with the Australian Government information security management protocol. The system should be able to detail the creation, location and destruction details of each document or file.

53. Agencies are to maintain a classified document register (CDR) for all TOP SECRET and ‘Accountable Material’ produced or received within an agency. The CDR should include details of the documents received and all retained copies. It is recommended that agencies have a register for SECRET information.

54. With due care a CDR should rarely need to be protectively marked. CDRs are to be protectively marked on their own merits and not according to the protective marking of the documents they record, unless the title of the document itself is protectively marked.

55. Where the volume of correspondence justifies it, separate registers for each security classification and inwards and outwards correspondence may be used.

4.2 Audit

56. Agencies are to develop an agency specific system for the audit of sensitive or security classified hardcopy information in accordance with the Australian Government information security management protocol.

57. Signing some form of receipt when sensitive or security classified information is delivered is a means of tracing the information’s movements, provides confirmation of receipt, and provides a level of assurance that the recipient will be responsible for the protection of that information.

58. Any type of receipt mechanism is suitable, as long as it identifies the document either by reference number or by title. A reference number is often easier when the title of a document is security classified. Agencies should specify a period on the receipt—for example, 14 days—in which the receipt is to be signed and returned by the recipient. Agencies are to confirm audit receipt returns within a month from the due date of their return.

59. For further details for the control and handling of security classified documents and material refer to the tables at the end of this guideline.

60. Agencies are to develop policies and procedures for the control and handling of all other official information in accordance with the Australian Government information security management protocol.

4.3 Spot checks

61. At irregular intervals the manager responsible for the information is to conduct, or arrange for a nominated officer to conduct, a spot check of a small sample of TOP SECRET files to ensure they are accounted for and are being handled, stored, etc in accordance with these guidelines.
62. It is recommended that spot checks be conducted on 5 per cent of TOP SECRET files per month, with 100 per cent of TOP SECRET files checked within every two-year period.

63. It is considered good security practice to conduct a similar spot check of other security classified files at irregular intervals.

64. The manager should report any discrepancy to the ASA for investigation.

4.4 Physical files holding protectively marked information

65. A file is to carry, as a minimum, the protective marking of the highest level of security classified information it holds. When new information is added to the file, the file user is to ensure that the protective marking carried by the file is still appropriate. If the information to be added is at a higher security classification than the file itself, the file user is to reclassify the file before attaching the new document. Agencies should consider whether the file would require a higher security classification due to the aggregation of the information contained within this file.

66. Protectively marked information that can be filed—that is, documents—should be placed on an appropriate file as soon as possible after its creation or receipt. This is usually following registration. TOP SECRET and SECRET documents are to be placed in an appropriate file or cover immediately. The location of at least the TOP SECRET document is to then be recorded in the CDR.

67. It is recommended that agencies use file reference and folio numbering for protectively marked files to maintain a record of the information held on the file. It is also considered good practice to follow normal filing procedures such as recording the date and name of the person holding the file.

68. The protective marking of the file is to be clearly and easily identifiable and easily distinguished from other markings. There are preferred standard colours for file covers that should be used for security classified files. Agencies might have other requirements that preclude the use of the standard colour file covers.
69. The standard colour file covers are:

- **TOP SECRET**—post office red
- **SECRET**—salmon pink
- **CONFIDENTIAL**—green
- **PROTECTED**—green plus stripe*

*The recommended stripe colour is Pantone Process Yellow-2U. The stripe should run diagonally across the front and on the spine.

70. The standard colour file covers for all other protectively marked information is buff.

### 4.5 Storage of sensitive and security classified information

71. Agencies are to store sensitive and security classified information in accordance with the [Australian Government physical security management guidelines—Security Zones and risk mitigation control measures.](#)

### 4.6 Aggregation of protectively marked information

72. The protective marking of a file is to be at least as high as the most highly protectively marked document it encloses.
73. Certain compilations of protectively marked information may require an application of a higher protective marking to a file than its component parts because the compromise of the combined information would cause a greater damage. This is normally referred to as ‘aggregation’.

74. If the amount of protectively marked information relating to a previously unclassified file is negligible, another part to the file should be opened and the protectively marked information placed on it. The new part should then be protectively marked accordingly.

75. For further information on the aggregation of electronic information see the Australian Government information security management guidelines—Management of aggregated information.
5. Procedures for production and reproduction of protectively marked documents

5.1 General

76. To help control protectively marked information, agencies should keep copies to a minimum.

77. Protectively marked information should be reproduced only when necessary. Spare or spoilt copies should be destroyed immediately and in accordance with section 10 of these guidelines. This destruction is defined as ‘normal administrative practice’ in terms of the Archives Act and does not need specific permission from the National Archives of Australia.

78. To make copies of protectively marked information that has a copy number, the originating agency’s permission is required. It is preferable that any additional copies be provided by the originator.

79. Should the originator give permission for the receiving agency to copy the information, agencies should provide the proposed additional distribution to the originator. The originator will indicate the appropriate additional copy numbers which are to be clearly marked on the additional copies.

80. Agencies may decide whether they wish to follow similar procedures for other sensitive and security classified information. Please note that such procedures are essential to operate a classified registry.

5.2 Accountable Material

Once disseminated, Accountable Material is not to be copied or reproduced in any form. If additional copies are required they are to be requested from the original source.

Information is not to be extracted from Accountable Material without the permission of the originator.

5.3 Foreign government information (FGI)

81. The Australian Government protective security governance guidelines—Safeguarding foreign government information (FGI) which will be released shortly is to be followed for the reproduction of foreign government information.

5.4 Photocopiers, facsimile machines and similar devices

82. Machines copying or transmitting protectively marked documents should be located in an area where activity cannot be conducted unobserved.

83. Staff responsible for operating these machines should stay within the vicinity of the machine until the action is complete and remove the document immediately.

84. Agencies should be aware that photocopiers, facsimile machines and similar devices, known as multi-function devices (MFDs) may retain images of copied documents. Consult ASD (assist@asd.gov.au) for advice on the sanitisation of these and similar devices.
85. Devices that are connected to ICT systems cannot be used to copy documents protectively marked higher than the ICT system to which the device is connected. See the ISM for further advice.

86. Devices connected to public networks are not to be used to copy protectively marked documents as the information can remain in the machine and could subsequently be transmitted.

87. Protectively marked documents are not to be transmitted by facsimile unless that information is protected in accordance with the ISM.
6. Removal of protectively marked documents and material from agency premises

6.1 General

88. If agencies wish to allow protectively marked documents and material to be removed from their premises they are to establish policies and procedures to ensure they are protected.

89. Removal is only to be allowed when there is a definite need—for example, attendance at meetings or short-term work at home—and when appropriate protection can be maintained en route and at the final destination.

90. Given the security requirements for the storage and care of TOP SECRET information, its removal for short-term work at home is not permitted without prior approval from ASIO and the originating agency.

91. Agencies are to follow the Australian Government physical security management guidelines—Working away from the office for guidelines on security arrangements for regular and long-term home-based work.

6.2 Within Australia

92. The removal of protectively marked documents and material outside the secure or authorised work area requires approval and an audit trail is to be established for accountability purposes.

93. While agencies decide who can authorise removal of protectively marked documents and material, it can only be authorised by the manager or equivalent responsible for that information and material. A record is to be maintained of all removals at TOP SECRET and SECRET levels.

94. Before approval is given for removal of protectively marked documents and material, the person removing the documents and material is to be made aware of the risks involved and be prepared to accept responsibility for its safe custody. The authorising officer is to be satisfied that there are adequate arrangements for the safe custody of the documents and material and a genuine need exists.

95. ASIO has published the Security Equipment Guide No. 5 Briefcases for the Carriage of Security Classified Information to assist agencies select briefcases suitable for carrying security classified information. The SEGs are available to agency security advisers (ASAs) from the Protective Security Policy Community on GovDex, ASAs may contact pspf@ag.gov.au for access.

96. Where protectively marked documents are transported outside the agency in an approved briefcase, they should be placed in a translucent envelope within the briefcase. The briefcase is to be locked at all times and is to be kept under the personal protection of the custodian. To prevent key duplication, keys should not be left in the lock, even when the briefcase is empty and unlocked.

97. Electronic media, such as laptops and disks that have been used to process protectively marked classified information requires protection to the same degree as paper-based protectively marked information equivalent to the highest level of protectively marked information ever placed on the media until it is sanitised. See the ISM for further information.
98. Apart from any authorisation granted, protectively marked information cannot be taken home unless the custodian has the appropriate protective security arrangements at their place of residence.

99. Agencies are to follow the *Australian Government physical security management guidelines—Working away from the office* for guidelines on security arrangements for regular and long-term home-based work.

100. If the security of information required for meetings interstate cannot be guaranteed by the person attending that meeting—for example, when staying overnight in a hotel—it may be forwarded in advance by appropriate transfer arrangements to a regional or branch office. Where necessary, similar arrangements are to be made for its return. If this is impractical the ASA’s advice is required.

6.3 Outside Australia

101. Protectively marked information can be exposed to a far greater risk when it is taken outside Australia, requiring increased protective measures.

102. Special care is necessary when protectively marked information is taken overseas. Agencies should check with the Department of Foreign Affairs and Trade (DFAT) about the most appropriate method of despatch.

103. The removal of protectively marked material requiring safe hand outside Australia, up to a maximum weight of 32 kilograms per individual item, is organised by DFAT.

104. Even when people travelling overseas require information, it should travel separately via the DFAT courier service, unless the person has diplomatic courier status. Note that this includes any form of electronic media or equipment, such as laptops.

105. If the use of the DFAT courier service is not practical, the ASA should contact DFAT or ASIO-T4 to discuss alternative arrangements. This would include bulky items and items over 32 kilograms. ASAs may seek advice from ASIO-T4 - t4ps@t4.gov.au.
7. Procedures for the transfer of protectively marked information and material

7.1 General

106. The security measures required to protect protectively marked information and material during physical transfer will depend on any protective markings, where it is going from and to, and the method used.

107. Any person wishing to transfer protectively marked information and material to another person is to be sure the intended recipient has the appropriate ‘need-to-know’ and the required level of security clearance before the information and material is transferred.

108. General advice on the various transfer procedures of protectively marked information and material is set out below. Agencies should develop a policy based on these minimum measures as well as for information and material too large for the ‘double barrier’ principle. In this instance agencies should take appropriate measures for transfer.

7.2 Preparing protectively marked information for physical transfer

109. Protective measures are required for protectively marked information while in transit outside agencies. This can include agency approved briefcases, Security Construction and Equipment Committee (SCEC) approved satchels, seals, pouches or transit bags, or special enveloping procedures and transferral by hand between people with the appropriate security clearance or by authorised messengers.

110. A number of methods can be used, for instance, ‘double enveloping’, or the use of a single paper envelope in conjunction with an approved briefcase, satchel, pouch or transit bag, or ‘single use’ SCEC-approved envelopes.

111. Whatever the combination used, the inner barrier is to be tamper evident and the outer barrier is to obscure the nature of the information being transferred.

112. Agencies are to use a double barrier to transfer security classified documents securely outside an agency.

113. Protectively marked information should be addressed to a specific position, appointment or named individual. An alternative individual or appointment is to be provided for TOP SECRET information and may be provided in the case of other protectively marked information. The sender is to have determined that the addressee and alternative possess the required level of security clearance.

114. The transfer of protectively marked information within a discrete office environment can be done without any coverings—such as envelopes—when:

- the information is transferred directly between members of staff who have the appropriate level of clearance to access it and the ‘need-to-know’, and
- there is no opportunity for unauthorised personnel to view the information.

115. If there is a risk that an unauthorised person could view the information it is to be covered.
7.3 Process for double enveloping

116. Double enveloping is used to help protect the ‘need-to-know’ principle in the transfer of security classified information and accountable material.

117. Double enveloping is a method that provides evidence of tampering. As the name suggests, double enveloping consists of placing security classified information and accountable material in two sealed envelopes.

118. Agencies are to use double enveloping for all security classified information—PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET—when either delivering by hand or using a SCEC-endorsed courier.

119. Double enveloping of information or material bearing DLMs is at agency discretion dependent on the agency security risk management plan.

120. When transferring security classified information the sender is to specify the intended recipient’s name, designation and full street address. Agencies are not to send security classified information to a post office box.

121. Double enveloping is used in conjunction with receipts that:

- are enclosed with the classified documents
- identify the date/time of dispatch, dispatching officer’s name, and
- have a unique identifying number.

7.3.1 Outer envelope

122. The outer envelope is used in a similar way to normal mail envelopes and gives protection to the inner envelope.

123. The outer envelope is not to:

- display the protective markings of the document or
- use tamper evident seals.

124. The outer envelope is to display:

- the physical address of the recipient
- a distinct reference number—this may be the receipt number if the envelopes are not individually numbered
- name and signature of dispatching officer, and
- date of dispatch.
7.3.2 Inner envelope

125. The inner envelope is used to give evidence of tampering. In addition to what should be displayed on the outer envelope the inner envelope should:

- display the protective markings at the top and bottom, and front and back of the envelope, and
- be sealed with SCEC-approved tamper evident seals in such a way that covert entry to the envelope is countered.

7.3.3 Other methods

126. There are single use envelopes that have been approved by SCEC for use:

- as an inner envelope
- as an outer envelope when used to enclose a number of inner envelopes where initial delivery will be to a registry or similar, and
- as a single opaque envelope in place of a double envelope. This procedure is not to be used for security classified information or where it is likely that a person other than the addressee or alternate addressee will open the envelope.

127. There is also a range of multi-use satchels that may be used in some circumstances. Refer to the Security equipment evaluated product list for further details.
8. Methods of transfer

8.1 Safe hand

128. Carriage of protectively marked information by safe hand means that it is despatched to the addressee in the care of an authorised officer or succession of authorised officers who are responsible for its carriage and safekeeping.

129. At each handover a receipt is obtained showing at least the identification number of the package, the time and date of the handover, and the name and signature of the recipient.

130. The purpose of sending an article via safe hand is to establish an audit trail that allows the sender to receive confirmation that the addressee received the information.

131. To send information via safe hand:
   - it is to be enclosed in a double barrier, that is, double enveloped
   - it is to possess a unique identification number—generally, this will be a receipt number
   - a two-part receipt is to be placed in the inner envelope with the information—the addressee will keep one portion and sign and return the other to the sender
   - some form of record or receipt system is also to accompany the package, so that every handover is documented
   - information should be transported in an approved briefcase or mailbag—agencies are to refer to the Security equipment catalogue available from SCEC, and
   - information is never to be left unattended—except when placed in the cargo compartment of an aircraft.

8.2 Carriage by SCEC-endorsed commercial courier

132. As an alternative to safe hand procedures, a number of commercial courier services have been endorsed by SCEC to carry security classified information. ASIO-T4 Protective Security Group - t4ps@t4.gov.au can provide advice to ASAs on SCEC-endorsed commercial couriers.

133. Note that the special handling requirements that apply to some security classified information carrying caveats may preclude the use of a commercial courier. AUSTEO information is to be transferred according to its level of security classification. The requirements for other caveats are established by the controlling agency. If unsure which couriers are endorsed and to what level, contact the ASA.

134. For carriage by commercial courier, security classified information is to be double enveloped. The courier satchel itself when opaque can stand as the outer envelope. Envelopes and wrappings need to be robust to stand up to the wear and tear of transit.

135. Security classified information is not to be left unattended while awaiting pick-up by courier.

136. On arrival at the receiving registry or government office, delivery documentation should be checked to ensure that the dispatched items arrived within the expected timeframe. If there
has been an undue delay or if there is any sign of tampering, both the sending and receiving
ASAs should be notified.

137. Security classified information in courier vehicles may only be left unattended for very short
periods of time, in which case the vehicle is to be secured. Generally, security classified
information should not be dispatched by overnight courier on days before weekends or public
holidays unless the addressee is able to receive it the following day and secure it appropriately.

8.3 Bulky material

138. Generally, where the size and weight of material is such that it cannot be moved by safe hand
procedures or SSEC-endorsed commercial couriers, special precautions should be made to
ensure that the material is not compromised, lost or damaged in transit.

139. Advice should be sought from the ASA who may, in turn, obtain advice from ASIO-T4 on the
carriage of such material.

8.4 High risk unclassified material

140. Intrinsically valuable material such as drugs and money, etc. might need to be transferred.

141. In this case, agencies may use commercial courier services.

142. Care is to be taken to assess the bona fides, suitability and reliability of any courier service used
to perform such work.

143. Wherever possible, agencies should avoid drawing attention to the specific nature of the
material being moved. It could also be highly desirable in some circumstances to seal the
material or security clear the employees of the courier services directly involved in the
movement of the material.

144. Special arrangements, such as armed escorts, could also be necessary in some cases.

145. Agencies engaging the services of courier companies to carry these assets are to ensure relevant
jurisdictional legislation is met and that the physical security protection offered by the courier
company is suitable to mitigate against identified risks.
9. **Receiving protectively marked documents**

9.1 **General**

146. Agencies are to ensure that personnel who receive protectively marked documents are aware of their responsibilities and, where necessary, hold the appropriate security clearance.

147. Protectively marked documents should only be opened by the addressee or the alternative addressee. An agency head may, however, authorise a specified person or area to open all mail to perform information or security management functions.

148. In the case where someone other than the intended addressee is charged with its opening, agencies should adopt the normal practice of opening the outer envelope only. If needed, the inner envelope should only be opened in the presence of the addressee.

149. The recipient of a package containing security classified documents is to verify that the information was transferred by the appropriate means and verify that its seals and packaging are still intact—see the table at the end of this guideline.

150. Agencies are to report any breakages, signs of tampering, or inappropriate methods of transfer to the ASAs of both the receiving and sending agency. If the package was delivered by a SCEC-endorsed courier, SCEC is to be advised. The recipient is to check that the contents and their integrity are preserved—for example, check pages and table of contents—and sign and return any receipt accompanying the information. If a security classified document register is kept, the information is then registered.

9.2 **Foreign government information**

151. From time to time agencies may receive information originating from a foreign government source. Agencies are to follow the *Australian Government information security management guidelines—Safeguarding foreign government information* (FGI) for receiving such information.
10. Procedures for the destruction of protectively marked documents and ICT media

10.1 General

152. Protectively marked information can be compromised because of inappropriate destruction. Agencies are to use approved procedures to dispose of protectively marked information. It is important to note that any disposal of official records needs to be in accordance with the *Archives Act 1983* (Cth). This usually means under the provisions of a disposal authority issued by the National Archives of Australia (NAA). Agencies should contact the NAA if they require further information relating to the disposal of records.

153. Security classified information is not to be, under any circumstances, disposed of by garbage or recycling collection unless it has already been through a SCEC-approved destruction process, such as shredding.

154. Agency security advisers can seek advice from ASIO-T4 for routine or emergency destruction of security classified information.

10.2 Methods of destruction

155. The following are the usual methods of destruction of security classified information:

- **pulping**—transforming mass to a given size determined by a removable screen
- **burning**—in accordance with relevant environment protection restrictions
- **pulverisation**—using hammermills with rotating steel hammers to pulverise the material
- **disintegration**—using blades to cut and gradually reduce the waste particle to a given size determined by a removable screen, and
- **shredding**—using strip-shredders and crosscut shredders. Only crosscut shredders are approved for security classified information.

156. Agencies are to refer to the *Australian Government physical security management guidelines – security zones and mitigation control measures* for advice on destruction equipment.

157. Where the destruction method is shredding, and the information is security classified as SECRET or above, it is to be shredded in an approved Class A crosscut shredder.

158. Where the destruction method is shredding, and the information is security classified as CONFIDENTIAL or PROTECTED, then it is to be shredded in an approved Class B crosscut shredder.

159. The ASIO *PSC 143 Destruction of security classified information* provides advice to ASAs on the required particle sizes for paper-based information and ICT media. The ISM – controls provides advice on the required particle sizes for ICT media.

10.3 Garbage and recycling

160. Garbage, whether it is placed in a garbage hopper or other area for collection or delivered directly to a garbage disposal service, is extremely vulnerable. Only information that is public
sector information or has already undergone an approved destruction process such as shredding should be discarded in the agency’s general garbage.

161. Recycling or discarding intact documents does not serve the same purpose as document destruction and should only be used by an agency for public sector information disposal or when the information has already undergone some form of appropriate destruction such as shredding.

162. Agencies are required to develop their own policy for destruction of unclassified information bearing DLMs, after considering any agency-specific issues in accordance with their agency’s security risk management plan.

10.4 External destruction

163. Agencies may consider that it is necessary for the destruction of their protectively marked information to be undertaken by an external destruction service. Any decision to do so should be based on sound risk management on what service – that is, transport type, procedures, facility and equipment – is to be used.

164. Agencies are to make an assessment of external destruction services against ASIO—T4 Criteria—agency-assessed and approved destruction service before engaging the service to destroy security classified information. The assessment includes a review of the collection process, transport, facility, procedures and approved equipment. As an alternative, agencies may use a National Association for Information Destruction (NAID) AAA certified destruction service with endorsements as specified in PSC 167 External destruction of security classified information.

165. A listing of NAID AAA certified destruction services with endorsements as specified in PSC 167 External destruction of security classified information can be found on the NAID website. Information marked TOP SECRET, or Accountable Material should be destroyed within agency premises and only once the originating agency has been notified. The originators may also apply special conditions to the destruction of some protectively marked information which might prevent contracting out destruction.

166. It is recommended that agencies destroying unclassified paper-based information make an assessment of the destruction service against ASIO – T4 Criteria – agency-assessed and approved destruction service or use a NAID AAA certified destruction service with an endorsement as specified in PSC 167 External destruction of security classified information. Agencies are to determine the procedures that it and the destruction service will use to maintain an appropriate level of security throughout the collection, transportation and destruction of security classified information. Appropriate procedures include:

- the security classified information is not to be left unattended at any time, and the vehicle and storage areas are appropriately secured
- the destruction is to be performed immediately after the material has arrived at the premises
- destruction of the security classified information is to be witnessed by an agency representative, or
- destruction service staff are to have a security clearance to the highest level of security classified information being transported and destroyed, or appropriately security cleared agency staff are to escort and witness the destruction.
167. Classified waste bags and bins are not security containers therefore they are to receive appropriate protection during use and storage by the agency before collection. Classified waste bags and bins need to be stored according to the highest level of security classified information they contain.

168. Agencies and contractors may use a variety of methods for destruction. It is essential, however, that all equipment used for destruction is approved.

10.5 ICT media and equipment

169. Agencies are to refer to the ISM for information on the sanitisation and destruction of electronic media and equipment.

10.6 Microfiche and other photographic material

170. Security classified microfiche and other photographic material is to be destroyed using SCEC approved equipment. The ASIO PSC 143 Destruction of security classified information provides advice to ASAs on the required particle sizes for destruction of microfiche.
## Table: Control and handling of security classified documents and material

### TOP SECRET

#### PREPARATION AND HANDLING

**Marking**
- Centre of top and bottom of each page.
- Markings are to be in capitals, bold text and a minimum of 5 mm high—preferably in red.
- Paragraph classifications should appear in a consistent position in brackets at the end of each paragraph or in the left margin, adjacent to the first letter of the paragraph.

**Numbering**
- Page numbering essential.
- Copy numbering essential.

#### Filing
- Distinctive file cover, standard colour is post office red.

#### Classified document register
- Record is to be kept of incoming and outgoing material.
- All incoming documents are to be placed immediately in an appropriate file cover.
- Refer to the Administrative

#### REMOVAL AND AUDITING

**Removal of documents or files**
- Basis of real need, e.g., meeting.
- Is to be in personal custody of individual and kept in SCEC-endorsed container e.g., briefcase, pouch, bag.
- Removal is to be authorised by the manager (or equivalent) responsible for the resource.
- Advice from ASA should be sought when removing for business purposes such as meeting or conference. Alternative arrangements (e.g., send ahead by SAFEHAND) should be considered.

**Audits**
- It is essential to conduct audits at irregular intervals. People nominated to conduct spot checks are required to sight documents and acknowledge this in writing.
- This process should be carried out in conjunction with the owner of the

#### COPYING, STORAGE AND DESTRUCTION

**Copying**
- Is to be copy-numbered.
- People authorising the copying of TOP SECRET information are to record in the file bearing the original, details of the number of copies made and their distribution.
- To be kept to a minimum in keeping with operational requirements.
- Any safeguards imposed by the originating authority are to be strictly observed.

**Physical safe-keeping—minimum standards**
- Clear desk policy.
- Agencies are to refer to the [Australian Government physical security management guidelines — Security zones and risk mitigation control measures](#).

#### PHYSICAL TRANSFER

**Within a single physical location**
- Single opaque envelope indicating the classification of the information AND receipt required AND one of the following:
  - either passed by hand between people who have the appropriate clearance and ‘need-to-know’, OR
  - placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger.
- May also be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate clearance and ‘need-to-know’ and there is no opportunity for any unauthorised person to view the information.

**Disposal**
- Unless required for Archival purposes, TOP SECRET material should be destroyed as soon as possible once it is no longer required for operational purposes.
| Functions Disposal Authority for the disposal of an administrative function or refer to the agency specific records disposal to cover records of unique business functions. | Disclosure or access  
- Security clearance to Negative Vetting 2 and a 'need-to-know'.  
- Only in accordance with legislative and administrative requirements. | Paper waste only  
- Only agency-assessed and approved NAIS AAA certified destruction service with specific endorsement and approved equipment and systems are to be used.  
- As it is ‘Accountable Material’, under supervision of two officers cleared to the appropriate level that are to supervise the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate.  
- Note: once a record is created it cannot be destroyed unless in accordance with the Archives Act.  
ICT media and equipment  
- Is to undergo sanitisation or destruction in accordance with ISM. | Transfer between establishments within Australia  
- Double-enveloping required AND receipt required AND one of the following:  
  — placed in an approved briefcase, satchel or pouch and delivered direct by an authorised messenger, OR  
  — delivered by SCEC-endorsed safe hand courier.  
Outside Australia  
- Double enveloping required AND receipt required AND DFAT courier service required. |
<table>
<thead>
<tr>
<th><strong>PREPARATION AND HANDLING</strong></th>
<th><strong>REMOVAL AND AUDITING</strong></th>
<th><strong>COPYING, STORAGE AND DESTRUCTION</strong></th>
<th><strong>PHYSICAL TRANSFER</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Marking</strong></td>
<td><strong>Removal of documents or files</strong></td>
<td><strong>Copying</strong></td>
<td><strong>Within a single physical location</strong></td>
</tr>
<tr>
<td><strong>• Centre of top and bottom of each page.</strong></td>
<td><strong>• Basis of real need, e.g., meeting.</strong></td>
<td><strong>• May be prohibited by originator.</strong></td>
<td><strong>• Single opaque envelope indicating the classification, receipt at discretion of originator, and either:</strong></td>
</tr>
<tr>
<td><strong>• Markings are to be in capitals, bold text and minimum of 5 mm high (preferably red).</strong></td>
<td><strong>• Is to be in personal custody of individual and kept in SCEC-endorsed container e.g., briefcase, pouch, bag.</strong></td>
<td><strong>• To be kept to a minimum in keeping with operational requirements.</strong></td>
<td><strong>— passed by hand between people who have the appropriate security clearance and ‘need-to-know’, OR</strong></td>
</tr>
<tr>
<td><strong>• Paragraph classifications should appear in a consistent position in brackets at the end of each paragraph or in the left margin, adjacent to the first letter of the paragraph.</strong></td>
<td><strong>• Removal is to be authorised by the manager (or equivalent) responsible for the resource.</strong></td>
<td><strong>Physical safe-keeping—minimum standards</strong></td>
<td><strong>— placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger.</strong></td>
</tr>
<tr>
<td><strong>Numbering</strong></td>
<td><strong>For home-based work, agencies are to refer to the Australian Government physical security management guideline—Working away from the office.</strong></td>
<td><strong>Destruction</strong></td>
<td><strong>• May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate clearance and ‘need-to-know’ and there is no opportunity for any unauthorised person to view the information.</strong></td>
</tr>
<tr>
<td><strong>• Page numbering essential.</strong></td>
<td><strong>A written record of removal is to be maintained.</strong></td>
<td><strong>Paper waste only</strong></td>
<td><strong>Transfer between establishments within Australia</strong></td>
</tr>
<tr>
<td><strong>• Serial number if in series.</strong></td>
<td><strong>Audits</strong></td>
<td><strong>Only agency-assessed and approved or NAID AAA certified destruction service with specific endorsement and approved equipment and systems are to be used.</strong></td>
<td><strong>• Double-enveloping required AND receipt required AND one of the following:</strong></td>
</tr>
<tr>
<td><strong>Filing</strong></td>
<td><strong>Where a register is maintained, audits should be conducted at irregular intervals.</strong></td>
<td><strong>Personnel nominated to conduct spot checks are required to sight documents and acknowledge this in writing.</strong></td>
<td><strong>— placed in an approved briefcase, satchel or pouch and delivered direct by an authorised messenger.</strong></td>
</tr>
<tr>
<td><strong>• Distinctive file cover, standard colour is salmon pink.</strong></td>
<td><strong>This process should be carried out in conjunction with the owner of the information or resource.</strong></td>
<td><strong>If Accountable Material, under supervision of two officers cleared to the appropriate level who is to supervise the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate.</strong></td>
<td><strong>Note: once a record is created it cannot be destroyed unless in</strong></td>
</tr>
<tr>
<td><strong>Classified document register</strong></td>
<td><strong>Audits</strong></td>
<td><strong>Note: once a record is created it cannot be destroyed unless in</strong></td>
<td><strong>•</strong></td>
</tr>
<tr>
<td><strong>• Record should be kept of incoming and outgoing material.</strong></td>
<td><strong>Where a register is maintained, audits should be conducted at irregular intervals.</strong></td>
<td><strong>•</strong></td>
<td><strong>•</strong></td>
</tr>
<tr>
<td><strong>• All incoming documents are to be placed immediately in an appropriate file cover.</strong></td>
<td><strong>Personnel nominated to conduct spot checks are required to sight documents and acknowledge this in writing.</strong></td>
<td><strong>•</strong></td>
<td><strong>•</strong></td>
</tr>
<tr>
<td><strong>• If declared by the originator as Accountable Document or Material, it is to have both a reference and</strong></td>
<td><strong>This process should be carried out in conjunction with the owner of the information or resource.</strong></td>
<td><strong>•</strong></td>
<td><strong>•</strong></td>
</tr>
<tr>
<td><strong>•</strong></td>
<td>****</td>
<td><strong>•</strong></td>
<td>****</td>
</tr>
</tbody>
</table>
Where a register is kept, refer to the Administrative Functions Disposal Authority for the disposal of an administrative function or refer to the agency specific records disposal to cover records of unique business functions.

**Disclosure or access**
- Security clearance to Negative Vetting 1 or above and ‘need-to-know’.
- Only in accordance with legislative and administrative requirements.

**ICT media and equipment**
- Is to undergo sanitisation or destruction in accordance with ISM.

**Outside Australia**
- Double enveloping required, receipt required and carriage by DFAT courier service or other authorised officers required.

<p>| messenger, OR |
| — delivered by SCEC-endorsed overnight courier. |</p>
<table>
<thead>
<tr>
<th>PREPARATION AND HANDLING</th>
<th>REMOVAL AND AUDITING</th>
<th>COPYING, STORAGE AND DESTRUCTION</th>
<th>PHYSICAL TRANSFER</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Marking</strong></td>
<td><strong>Removal of documents or files</strong></td>
<td><strong>Copying</strong></td>
<td><strong>Within a single physical location</strong></td>
</tr>
<tr>
<td>Centre of top and bottom of each page.</td>
<td>Basis of real need, e.g., meeting.</td>
<td>May be prohibited by originator.</td>
<td>Single opaque envelope indicating the classification, receipt at discretion of originator, and either:</td>
</tr>
<tr>
<td>Markings are to be in capitals, bold text and a minimum of 5 mm high (preferably red).</td>
<td>Is to be in personal custody of individual and kept in SCEC-endorsed container e.g., briefcase, pouch, bag.</td>
<td>To be kept to a minimum in keeping with operational requirements.</td>
<td>— passed by hand between people who have the appropriate security clearance and ‘need-to-know’, OR</td>
</tr>
<tr>
<td>Paragraph classifications should appear in a consistent position in brackets at the end of each paragraph or in the left margin, adjacent to the first letter of the paragraph.</td>
<td>Removal is to be authorised by the manager (or equivalent) responsible for the resource.</td>
<td>Physical safe-keeping—minimum standards</td>
<td>— placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger.</td>
</tr>
<tr>
<td><strong>Numbering</strong></td>
<td><strong>For home-based work, refer to the Australian Government physical security management guideline—Working away from the office.</strong></td>
<td><strong>Clear desk policy.</strong></td>
<td><strong>May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate clearance and ‘need-to-know’ and there is no opportunity for any unauthorised person to view the information.</strong></td>
</tr>
<tr>
<td>Page or paragraph numbering desirable.</td>
<td><strong>Audits</strong></td>
<td><strong>Agencies are to refer to the Australian Government physical security management guidelines—Security zones and risk mitigation control measures.</strong></td>
<td><strong>Transfer between establishments within Australia</strong></td>
</tr>
<tr>
<td><strong>Filing</strong></td>
<td><strong>It is good security practice to implement spot checks of information at this level.</strong></td>
<td><strong>Destruction</strong></td>
<td><strong>EITHER:</strong></td>
</tr>
<tr>
<td>Distinctive file cover, standard colour is green.</td>
<td><strong>Paper waste only</strong></td>
<td><strong>Accountable Material, under supervision of two officers cleared to the appropriate level who are to supervise the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate.</strong></td>
<td>— Single opaque envelope that does not give any indication of the classification AND placed in an approved briefcase, satchel or pouch and delivered direct, by</td>
</tr>
<tr>
<td>** Classified document register**</td>
<td><strong>Only agency-assessed and approved or NAID AAA certified destruction service with specific endorsement and approved equipment and systems are to be used.</strong></td>
<td><strong>Note: once a record is created it cannot be destroyed unless in</strong></td>
<td>** approved briefcase, satchel or pouch and delivered direct, by**</td>
</tr>
<tr>
<td>It is good security practice to keep a record of incoming and outgoing information.</td>
<td><strong>If Accountable Material, under supervision of two officers cleared to the appropriate level who are to supervise the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate.</strong></td>
<td><strong>Transfer between establishments within Australia</strong></td>
<td><strong>approved briefcase, satchel or pouch and delivered direct, by</strong></td>
</tr>
<tr>
<td>Where a register is kept, refer to the Administrative Functions Disposal Authority for the disposal of an administrative function or refer to the agency specific records disposal to cover records of unique business activities.</td>
<td><strong>Note: once a record is created it cannot be destroyed unless in</strong></td>
<td><strong>Transfers between establishments within Australia</strong></td>
<td><strong>approved briefcase, satchel or pouch and delivered direct, by</strong></td>
</tr>
<tr>
<td><strong>functions.</strong></td>
<td><strong>ICT media and equipment</strong></td>
<td><strong>Outside Australia</strong></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>• If declared by the originator as Accountable Document or Material, it is to have both a reference and copy number.</td>
<td>• Is to undergo sanitisation or destruction in accordance with ISM.</td>
<td>• Double enveloping required, receipt required and carriage by DFAT courier service or other authorised officers required.</td>
<td></td>
</tr>
<tr>
<td><strong>Disclosure or access</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security clearance to Negative Vetting 1 or above and ‘need-to-know’.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Only in accordance with legislative and administrative requirements.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PREPARATION AND HANDLING</td>
<td>REMOVAL AND AUDITING</td>
<td>COPYING, STORAGE AND DESTRUCTION</td>
<td>PHYSICAL TRANSFER</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------</td>
<td>----------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Marking</td>
<td>Removal of documents or files</td>
<td>Copying</td>
<td>Within a single physical location</td>
</tr>
<tr>
<td>• Centre of top and bottom of each page.</td>
<td>• Basis of real need, e.g., meeting.</td>
<td>• May be prohibited by originator.</td>
<td>• Single opaque envelope that indicates the classification, receipt at discretion of originator, and either:</td>
</tr>
<tr>
<td>• Markings are to be in capitals, bold text and a minimum of 5 mm high (preferably red).</td>
<td>• Is to be in personal custody of individual and kept in SSEC-endorsed container e.g., briefcase, pouch, bag.</td>
<td>• To be kept to a minimum in keeping with operational requirements.</td>
<td>— passed by hand between people who have the appropriate security clearance and ‘need-to-know’, OR</td>
</tr>
<tr>
<td>• Paragraph classifications should appear in a consistent position in brackets at the end of each paragraph or in the left margin, adjacent to the first letter of the paragraph.</td>
<td>• Removal is to be authorised by the manager (or equivalent) responsible for the resource.</td>
<td>Physical safe-keeping—minimum standards</td>
<td>— placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger.</td>
</tr>
<tr>
<td>Numbering</td>
<td>• For home-based work, refer to the <a href="#">Australian Government physical security management guideline—Working away from the office</a>.</td>
<td>Clear desk policy.</td>
<td>May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between members of staff with the appropriate clearance and ‘need-to-know’ and there is no opportunity for any unauthorised person to view the information.</td>
</tr>
<tr>
<td>• Page or paragraph numbering desirable.</td>
<td>Audits</td>
<td>Agencies are to refer to the <a href="#">Australian Government physical security management guidelines—Security zones and risk mitigation control measures</a>.</td>
<td>Transfer between establishments within Australia</td>
</tr>
<tr>
<td>Filing</td>
<td>• It is good security practice to implement spot checks of information at this level.</td>
<td>Destruction</td>
<td>EITHER:</td>
</tr>
<tr>
<td>• Distinctive file cover, standard colour is green with yellow stripe.</td>
<td>Paper waste only</td>
<td></td>
<td>• Single opaque envelope that does not give any indication of the classification AND placed in an approved briefcase, satchel or</td>
</tr>
<tr>
<td>Classified document register</td>
<td>• Only agency-assessed and approved or NAID AAA certified destruction service with specific endorsement and approved equipment and systems are to be used.</td>
<td></td>
<td>pouch and should be moved directly to the point of destruction.</td>
</tr>
<tr>
<td>• It is good security practice to keep a record of incoming and outgoing information.</td>
<td>• If Accountable Material, under supervision of two officers cleared to the appropriate level who are to supervise the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate.</td>
<td></td>
<td>Only single item per envelope.</td>
</tr>
<tr>
<td>• Where a register is kept, refer to the Administrative Functions Disposal Authority for the disposal of an administrative function or refer to the agency specific records disposal</td>
<td>• Note: once a record is created it</td>
<td>Transfer between establishments outside Australia</td>
<td></td>
</tr>
</tbody>
</table>
to cover records of unique business functions.

- If declared by the originator as Accountable Document or Material, it is to have both a reference and copy number.

**Disclosure or access**

- Security clearance to Baseline or above and ‘need-to-know’.
- Only in accordance with legislative and administrative requirements.

<table>
<thead>
<tr>
<th>ICT media and equipment</th>
<th>cannot be destroyed unless in accordance with the Archives Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Is to undergo sanitisation or destruction in accordance with ISM.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>pouch and delivered direct, by hand, by an authorised messenger AND receipt required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OR</strong></td>
</tr>
<tr>
<td>- Double enveloping AND receipt required AND delivered by SCEC-endorsed overnight courier.</td>
</tr>
</tbody>
</table>

**Outside Australia**

- Double enveloping required, receipt required and carriage by DFAT courier service or other authorised officers required.