# Guide to Labelling Sensitive Information

## Document Ownership Information

<table>
<thead>
<tr>
<th>Document Owner</th>
<th>J Albani</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Preparation</td>
<td></td>
</tr>
<tr>
<td>Document Confidentiality</td>
<td></td>
</tr>
</tbody>
</table>

## Document Name and Version Control
*(Circulated versions only)*

<table>
<thead>
<tr>
<th>Document Name &amp; Location</th>
<th><a href="http://www.services.nsw.gov.au">www.services.nsw.gov.au</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td><strong>Date</strong></td>
</tr>
</tbody>
</table>
| 1.0  
(First Release) | October 2002 | | First release based on drafts and feedback from reviewers. |
| 1.1 | March 2011 | T Sarkar | Updated template and removed GCIO references |
| 1.2 | June 2011 | D Anspal | Changed contact details |
# Table of Contents

1. Overview .................................................................................................................. 1  
2. Introduction ............................................................................................................... 2  
3. Applicability ............................................................................................................ 3  
4. Definitions ............................................................................................................... 4  
5. Points to note .......................................................................................................... 5  
6. X-IN-CONFIDENCE .............................................................................................. 7  
7. Protected ............................................................................................................... 10  
8. Highly Protected .................................................................................................... 13
1. **Overview**

There is an obvious need to protect sensitive official information from unauthorised access. Accordingly all NSW Government Agencies should use 'Labels' to mark such information, whether it is in electronic, paper or some other Form.

Strict adherence to the standard labelling procedures detailed in this Guide will ensure confidentiality and consistent safeguards for sensitive information that is distributed among NSW Government agencies or wholly within an agency.

There are three levels of label. In ascending order of sensitivity these are:

- X-IN-CONFIDENCE where ‘X’ may be ‘CABINET’, ‘COMMERCIAL’,
- 'CLIENT', 'PERSONNEL' or some other term selected by an agency as appropriate to their needs;
- PROTECTED;
- HIGHLY PROTECTED.

The Guide provides examples of each level of sensitivity and gives clear guidelines on preparing and handling; removal and auditing; copying, storage and disposal; and transmission of such materials.

An agency receiving information with a sensitivity label must treat it according to this Guide.

The absence of a sensitivity label means that official information continues to be handled in accordance with existing practices, including compliance with the Government Information (Public Access) Act 2009 (GIPA Act).
2. Introduction

The use of standard labels to mark sensitive official information, whether in electronic, paper or some other form, means that these documents can be distributed among NSW Government agencies and be subject to consistent safeguards in all of them. This Guide specifies minimum recommended requirements for such labelling and is based on the 'Commonwealth Protective Security Manual', 2000 (PSM) which has been superseded Australian Government Protective Security Policy Framework.

The Guide establishes three levels of sensitive information and rules for handling them to protect confidentiality. In some instances (particularly information in Electronic form) the labels may also indicate a need for additional measures to safeguard integrity and ensure availability.

Some agencies will already have labelling and security procedures. They may tailor the Guide to meet their own internal needs based on any existing procedures, their own risk assessment and having regard to the minimum standards set out in the Guide. Documents sent to other agencies, however, must be labelled strictly according to the Guide.

Some agencies hold classified information from the Commonwealth in Accordance with Commonwealth requirements. This Guide does not alter these requirements.

It is expected that the Guide will assist agencies in safeguarding information in accordance with the Privacy and Personal Information Protection Act. Normal procedures apply to handling official information that does not have a sensitivity label.
3. Applicability

When an agency's security policies establish a need for sensitivity labels, the labels and practices specified in this Guide should be used. This Guide may be appropriately amplified in agencies’ procedures. Agencies must not create their own labelling schemes.

An agency sending sensitive information to another Government agency must label the information in accordance with this Guide and an agency receiving information with a sensitivity label must handle it according to this Guide.
4. Definitions

The term 'need to know' means that access to information should be limited to those that need to know or use it. It is applied at the level of specific individuals and applies to all types of sensitive information.

In this Guide the term 'accountable' means particularly sensitive information requiring strict access and movement control. Such items are recorded in a register in each holding organisation.

The term 'clear desk policy' means that items with sensitive (X-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED) labels must be secured when unattended and their content always unobservable to people without the 'need to know'.

The term 'infrequent' means no more than one transmission per month within or from a site.

The term 'secure area' means a work area to which physical access is controlled and all visitors, whether working for the agency or not, are escorted. A 'secure area' would be inside the outer protection of a controlled entry building or office area.

The term 'double enveloping' means using two opaque sealed envelopes, one inside the other, the inner one being signed and office stamped by the sender and having all edges adhesive taped. The outer envelope must not indicate the sensitivity of the contents.
5. Points to note

The three levels of label are, in ascending order of sensitivity:

- X-IN-CONFIDENCE where ‘X’ may be ‘CABINET’, ‘COMMERCIAL’, ‘CLIENT’, ‘PERSONNEL’ or some other term selected by an agency as appropriate to their needs;
- PROTECTED;
- HIGHLY PROTECTED.

‘Need to know’ is the governing principle for access to all sensitive information. However, ‘need to know’ or the use of a sensitivity label does not alter or override any part of the Freedom of Information Act (or any other legislation) and the public right to information, but indicates that particular care is required in reviewing information for release.

A label may be removed or downgraded when the information is no longer sensitive. When this is known in advance (e.g., an announcement date or specific event) then the label should be annotated with the downgrading date.

The measures detailed in this Guide are based on the assumption that only small amounts of PROTECTED and HIGHLY PROTECTED information are held by most NSW agencies. ‘Over classification’ is often a problem and to help minimise this, the originator of a PROTECTED or HIGHLY PROTECTED item must obtain the approval of a supervisory person for the label's use.

The Privacy and Personal Information Protection Act requires agencies to take reasonable security measures to protect personal information. Section 19 of the Act defines certain items of personal information as sensitive. It would be appropriate to label information containing one or more of these sensitive items as X-IN-CONFIDENCE.

The State Records Authority of NSW has produced a series of Standards and Guidelines that provide additional information concerning transmission, storage and disposal of records, public access to records and the use of record keeping metadata. The NSW Record Keeping Metadata standard recommends that access restrictions and use of information is kept for State records in all forms, to ensure their proper and authorised access and use. More information is available from State Records. Note that records are a class of official information and metadata is information about any type of information.

When courier services are required, only those endorsed by the Commonwealth's Security Construction and Equipment Committee (SCEC) are to be used for sensitive information. For PROTECTED and HIGHLY PROTECTED material a ‘Safe Hand’ level of service must be used.

The Commonwealth has various classes of security container manufactured to ASIO approved specifications for PROTECTED and HIGHLY PROTECTED items in variously secure environments. These classes of security container have not been specified in this Guide but agencies may consider it appropriate to use them. Details are in the PSM.

The PSM directs that specific colours of file cover be used for different sensitivity labels. This Guide does not require such an approach. However, agencies are strongly recommended to reserve particular file cover colours for particular sensitivity labels as an aid to ensuring that sensitive information is not inadvertently mishandled.

Reference is made to the Commonwealth publication Australian Communications-Electronic Security Instruction (ACSI) 33 - ‘Security Guidelines for Australian Government IT Systems’ for security in an electronic environment.

This should be used as a guide where it is referenced and may be used where an agency's risk management indicates that stronger measures than those outlined in this Guide are needed.
Guide to Labelling Sensitive Information

The Australian Business Number - Digital Signature Certificate (ABN-DSC) is a class of public key certificate approved by the Commonwealth that may be used within and between agencies and with business. States and Territories have agreed to use ABN-DSC when appropriate. It has two key pairs; one (authentication keys) for digital signatures the other (confidentiality keys) for content encryption. The confidentiality keys are appropriate to encrypt X-IN-CONFIDENCE information, and infrequent and unpredictable transmission of PROTECTED or HIGHLY PROTECTED information.

As a general principle ICT security products should only be selected if they have been evaluated to Common Criteria (ISO 15408) or similar older standards.

Where X-IN-CONFIDENCE information is involved, assurance level EAL4 or equivalent would be the minimum acceptable level. Appropriate products are available through State Contracts Control Board panel contract ITS2319, including items from the Defence Signals Directorate’s (DSD) Evaluated Products List (EPL).

Where official information is stored in encrypted form, suitably secure arrangements must be made to ensure that it can be made available in the event of key loss.

This Guide does not provide complete technical details for a secure ICT environment. This is a matter for agency ICT security plans, which must reflect current and appropriate good practice. In particular, while firewalls are specified they are only one part of a trustworthy ‘defence’. Furthermore effective ICT security requires all measures to be properly documented and maintained under formal configuration management, including periodic audit.
Guide to Labelling Sensitive Information

6. X-IN-CONFIDENCE

(e.g. COMMERCIAL-IN-CONFIDENCE, CABINET-IN-CONFIDENCE, PERSONNEL-IN-CONFIDENCE and others a appropriate)

6.1 Examples of X-IN-CONFIDENCE material

- Information whose compromise could cause limited damage to NSW, the Government, commercial entities or members of the public, e.g.:
- Cause substantial distress to individuals or private entities;
- Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or private entities;
- Prejudice an investigation;
- Facilitate the commission of crime;
- Breach proper undertakings to maintain the confidence of information provided by third parties;
- Impede the effective development or operation of Government policies;
- Breach statutory restrictions on disclosure of information;
- Disadvantage the Government in commercial or policy negotiations with others;
- Undermine the proper management of the public sector and its operations.

6.2 Preparation and handling

Marking:

- Centre of top and bottom of each page;
- Markings should be in capitals, bold text and a minimum of 5mm high (preferably red stamp);
- The label on a file cover must be at least equal to the label on the most sensitive item in the file;
- Paragraph classifications, where adopted, should appear in a consistent position such as in the left margin adjacent to the first letter of the paragraph;
- Electronic and other documents must include their sensitivity label in their metadata.

Numbering:

- Page and / or paragraph numbering is desirable.

Filing & Media Labels:

- Front and back file covers & media labels to be marked 'X-IN-CONFIDENCE' in large letters;
- An agency may reserve specific colours for file covers and media labels covering 'X-IN-CONFIDENCE' items.
Guide to Labelling Sensitive Information

Sensitive Document Register:
- No special requirement;
- A register is not to disclose sensitive titles of documents to staff without the 'need to know'.

Disclosure / access:
- Need to know;
- Only in accordance with legislative and administrative requirements.

6.3 Removal and auditing

Removal of documents or files:
- Basis of real need, e.g., a meeting;
- Removal must be authorised by a supervisor (or equivalent) who should be satisfied that the removing officer is aware of the potential risks involved and that he or she is responsible for its safe custody at all times;
- Ensure adequate custodial arrangements, including overnight storage.

Audits:
- Not essential for security purposes.

6.4 Copying, storage and disposal

Copying
- May be prohibited by originator;
- Copying of 'CABINET-IN-CONFIDENCE' is always prohibited;
- To be kept to minimum in keeping with operational requirements.

Physical safe-keeping — minimum standards
- 'Clear desk' policy;
- Hard copy and any form of unencrypted removable electronic media must be held in a commercial grade locked container or a secure area;
- Servers and associated devices processing or storing X-IN-CONFIDENCE data must be sited in appropriately secure facilities. ACSI 33 provides a guide.

Electronic Storage
- X-IN-CONFIDENCE information must be encrypted using an encryption method approved by the agency ICT security plan when stored in any laptop or on a non-removable PC hard drive.

Disposal
- Transfer in accordance with the State Records Act; or if not required then:
  - paper items only: destroy by appropriate method or contract approved in the agency security plan; or
  - for all other media: consult information security officer.
Guide to Labelling Sensitive Information

Note: State records in any form may only be disposed of in accordance with Part 3 of the State Records Act, 1998.

6.5 Manual transmission

Within a single physical location
Single sealed opaque envelope that indicates the sensitivity label of the information, delivered by agency's internal mail system.

- May be passed, uncovered, by hand within a secure area provided it is transferred directly between people with the need to know and there is no opportunity for any unauthorised person to view the information.

Transfer between establishments
Single sealed opaque envelope that does not indicate the sensitivity label of the information; receipt at discretion of originator AND one of the following:

- Passed by hand between people who have the need to know;
- Delivered by a SCEC endorsed overnight courier;
- Delivered by Australia Post, State Mail Service or DX service.

6.6 Electronic transmission

Telephone, facsimile and video conference equipment

- Information may be passed unencrypted over an agency's private communications system provided it is contained within a single site and uses only wire line or fibre optic bearers (that is, with no microwave, cellular telephone, wireless LAN or similar radio frequency links).
- Between sites or within sites using other than wire line or fibre optic transmission, information should be encrypted and must be encrypted if its transmission is regular or frequent.

Data transmissions and e-mail

- Infrequent transmissions may be made without special controls;
- Regular or frequent traffic must be encrypted. Suitable e-mail encryption products can be found in DSD's Evaluated Products List.

Computer networks

- May only be connected to public networks (including Internet) via firewalls on DSD's Evaluated Products List.
7. **Protected**

This sensitivity label will rarely be necessary. An originator is not to apply it without the approval of their supervisor or similar person.

7.1 **Examples of PROTECTED material**

Information whose compromise could cause damage to NSW, the Government, commercial entities or members of the public, e.g.

- Endanger individuals and private entities;
- Work substantially against state or national finances or economic or commercial interests;
- Substantially undermine the financial viability of major organisations
- Facilitate the commission of serious crime;
- Seriously impede the development or operation of major Government policies.

7.2 **Preparation and handling**

**Marking**

- Centre of top and bottom of each page;
- Markings should be in capitals, bold text and a minimum of 10mm high (preferably red stamp);
- The label on a file cover must be at least equal to the label on the most sensitive item in the file;
- Paragraph classifications, where adopted, should appear in a consistent position such as in the left margin adjacent to the first letter of the paragraph;
- Electronic and other documents must include their sensitivity label in their metadata.

**Numbering**

- Page numbering is essential & paragraph numbering desirable.

**Filing & Media Labels**

- Front and back file covers & media labels to be marked ‘PROTECTED’ in large letters;
- An agency may reserve a specific colour for file covers and media labels covering ‘PROTECTED’ items.

**Sensitive document register**

- It is good security practice to keep a record of incoming and outgoing information;
- If declared by the originator as 'Accountable Document / Material', it must have both a reference and copy number;
- A register is not to disclose sensitive titles of documents to staff without the 'need to know'.
Disclosure / access

- Need to know;
- Only in accordance with legislative and administrative requirements.

7.3 Removal and auditing

Removal of documents or files

- Basis of real need, e.g., a meeting;
- Must be in personal custody of individual and when not in use kept in a locked container;
- Removal must be authorised by a manager (or equivalent) responsible for the business unit that is custodian of the information.

Audits

- It is good security practice to establish a program of spot checks of information at this level.

7.4 Copying, storage and disposal

Copying

- May be prohibited by originator;
- To be kept to a minimum in keeping with operational requirements.

Physical safe-keeping-minimum standards

- Clear desk policy;
- Hard copy and any form of unencrypted removable electronic media must be kept in a locked container in a secure area;
- Servers and associated devices processing or storing PROTECTED data must be sited in appropriately secure facilities. ACSI 33 provides a guide.

Electronic Storage

- PROTECTED information must be encrypted using an encryption method approved by the agency security plan when stored in any laptop or on a non-removable PC hard rive.

Disposal

- Transfer in accordance with the State Records Act; or if not required then:
  - paper items only: destroy by shredding;
  - Electronic media and equipment: must undergo sanitisation in accordance with ACSI 33;
  - If ‘accountable material’; under supervision of two officers who must supervise the removal of the material to the point of destruction, ensure that destruction is complete and sign a destruction certificate.

Note: State records in any form may only be disposed of in accordance with Part 3 of the State Records Act, 1998.
Guide to Labelling Sensitive Information

7.5 Manual transmission

Within a single physical location

Single opaque envelope that indicates the classification; receipt at discretion of originator AND:

- Either passed by hand between people who have the need to know;
- Or placed in locked container and delivered direct, by hand, by an authorised messenger;
- May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between members of staff with the need to know and there is no opportunity for any unauthorised person to view the information.

Transfer between establishments

- Either single opaque envelope that does not give any indication of the classification AND placed in a locked container and delivered direct, by hand, by an authorised messenger AND receipt required;
- Or double enveloping AND receipt required AND delivered by a SCEC endorsed overnight courier using the ‘Safe Hand’ level of service.

7.6 Electronic transmission

Telephone, facsimile and video conference equipment

- Information may be passed in clear over an agency's private communications system contained within a single site, using wire line or fibre optic bearers having a low probability of interception or where PROTECTED traffic is unpredictable & infrequent;
- Between or within sites using other than wire line or fibre optic bearers, unless there is a low probability of interception and PROTECTED traffic is unpredictable & infrequent, information must be encrypted using products from DSD's Evaluated Products List.

Data transmissions and e-mail

- Unpredictable & infrequent PROTECTED transmissions may be made without special controls. Otherwise agencies must use encryption products from DSD's Evaluated Products List.

Computer networks

- Can only be connected to public networks (including Internet) via firewalls from DSD's Evaluated Products List.
8. Highly Protected

This sensitivity label will only be necessary for exceptional items. An originator is not to apply it without the approval of a senior manager.

8.1 Examples of HIGHLY PROTECTED material

Information whose compromise could cause serious damage to NSW, the Government, commercial entities or members of the public e.g.

- Threaten life directly;
- Seriously prejudice public order;
- Substantially damage state or national finances or economic and commercial interests.

8.2 Preparation and handling

Marking

- Centre of top and bottom of each page;
- Marking should be in capitals, bold text and a minimum of 10mm high (preferably red stamp);
- The label on a file cover must be at least equal to the label on the most sensitive item in the file;
- Paragraph labels, where adopted, should appear in a consistent position such as in the left margin adjacent to the first letter of the paragraph;
- Electronic or other documents must include their sensitivity label in their metadata.

Numbering

- Page numbering is essential & paragraph numbering highly desirable;
- Copy numbers must be used.

Filing & Media Labels

- Front and back file covers & media labels to be marked 'HIGHLY PROTECTED' in large letters;
- An agency may reserve a specific colour for file covers and media labels covering 'HIGHLY PROTECTED' items.

Sensitive document register

- Record should be kept of incoming and outgoing material;
- All incoming documents must be placed without delay in an appropriate file cover;
- If declared by the originator as 'Accountable Document / Material', it must have both a reference and copy number;
- A register is not to disclose sensitive titles of documents to staff without the 'need to know'.
Guide to Labelling Sensitive Information

Disclosure / access
- Need to know;
- Only in accordance with legislative and administrative requirements.

8.3 Removal and auditing

Removal of documents or files
- Basis of real need, e.g. a meeting;
- Must be in personal custody of individual and kept in a locked container;
- Removal must be authorised by the manager (or equivalent) responsible for the business unit that is custodian of the information;
- A written record of removal must be maintained.

Audits
- Where a register is maintained, audits must be conducted at irregular intervals;
- Personnel 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 custodian of the information / resource.

8.4 Copying, storage and disposal

Copying
- May be prohibited by originator;
- To be kept to a minimum in keeping with operational requirements, each copy numbered.

Physical safe-keeping - minimum standards
- Clear desk policy;
- Hard copy and any form of unencrypted removable electronic media must be held in a safe in a secure area;
- Servers and associated devices processing or storing HIGHLY PROTECTED data must be sited in appropriately secure facilities. ACSI 33 provides a guide.

Electronic Storage
- HIGHLY PROTECTED information must be encrypted using an encryption method approved by the agency security plan when stored in any laptop or on a non-removable PC hard drive.

Disposal
- Transfer in accordance with the State Records Act; or if not required then:
  - paper items only: destroy by shredding in a two axis shredder; or
  - electronic media and equipment: must undergo sanitisation in accordance with ACSI 33;
  - if ‘accountable material’; under supervision of two officers who must supervise the removal of the material to the point of destruction, ensure that destruction is complete and sign a destruction certificate.
Guide to Labelling Sensitive Information

*Note:* State records in any form may only be disposed of in accordance with Part 3 of the State Records Act, 1998.

### 8.5 Manual transmission

**Within a single physical location**

Single sealed opaque envelope that indicates the classification; receipt at discretion of originator AND:

- Either passed by hand between people who have the need to know;
- Or placed in a locked container and delivered direct, by hand, by an authorised messenger;
- May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between members of staff with the need to know and there is no opportunity for any unauthorised person to view the information.

**Transfer between establishments**

Double-enveloping required AND receipt required AND:

- Either placed in a locked container and delivered direct by an authorised messenger;
- Or delivered by a SCEC endorsed overnight courier using a 'Safe Hand' level of service.

### 8.6 Electronic transmission

**Telephone, facsimile and video conference equipment:**

- Information may be passed in clear over an agency's private communications system contained within a single site using wire line or fibre optic bearers where the probability of interception is negligible;
- Between and within sites using other than wire line or fibre optic bearers, unless the probability of interception is negligible and PROTECTED and HIGHLY PROTECTED traffic is unpredictable and infrequent, information must be encrypted using products from DSD's Evaluated Products List.

**Data transmissions and e-mail**

- If PROTECTED and HIGHLY PROTECTED traffic is unpredictable & very infrequent, HIGHLY PROTECTED transmissions may be made without special controls. Otherwise agencies shall utilise encryption products from DSD's Evaluated Products List.

**Computer networks**

- Should only be connected to public networks (including Internet) via two different firewalls from DSD's Evaluated Products List and supported by intrusion detection with 24 x 7 immediately reactive procedures.