Identification

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Information Protection Guidelines</td>
</tr>
<tr>
<td>Document No:</td>
<td>D14/412274</td>
</tr>
<tr>
<td>Business Centre:</td>
<td>Information Technology Services</td>
</tr>
<tr>
<td>Governance Area:</td>
<td>Service Design</td>
</tr>
<tr>
<td>Process:</td>
<td>Information Management</td>
</tr>
<tr>
<td>Owner:</td>
<td>Director, ITS Governance</td>
</tr>
<tr>
<td>Date of Effect:</td>
<td>August 2014</td>
</tr>
<tr>
<td>Contact:</td>
<td>Manager, Information Security</td>
</tr>
<tr>
<td>Next Review:</td>
<td>August 2015</td>
</tr>
<tr>
<td>Classification:</td>
<td>Unclassified</td>
</tr>
</tbody>
</table>

Acceptance

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS Governance:</td>
<td>Joy Gault</td>
<td></td>
<td>12 August 2014</td>
</tr>
<tr>
<td>Document Owner:</td>
<td>James Spring</td>
<td></td>
<td>14 August 2014</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Review by</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Aug 2014</td>
<td>Derek.Winter</td>
<td>Final Draft</td>
</tr>
<tr>
<td>29 Jul 2014</td>
<td>Satoshi.Yasuda</td>
<td>Draft</td>
</tr>
</tbody>
</table>

Printed copies of this document may not be up to date. Ensure you have the latest version before using this document.
Table of Contents

1 Introduction 3

2 Scope 3

3 Purpose 3

4 Information Protection 4

4.1 Labelling 4

4.1.1 Interaction with Legislation 4

4.1.2 Unlabelled Information 4

4.1.3 Applying Protective Markings 4

4.1.4 Labelling Paper (hard copy) Documents 5

4.1.5 Labelling Electronic documents 5

4.2 Removal 5

4.3 Sharing 6

4.3.1 Receiving Commonwealth Information 6

4.3.2 Information Shared with External Agencies or Third Parties 7

4.4Copying 8

4.4.1 Approval from originator 8

4.4.2 Spare copies 8

4.4.3 Copy number 9

4.4.4 Copiers, Printers and Multi-Function Devices (MFDs) 9

4.5 Storage 10

4.5.1 Physical safe-keeping 10

4.5.2 Laptop and removable media 10

4.6 Disposal 10

4.6.1 Paper items 10

4.6.2 Other Media 11

4.7 Electronic Transmission 11

4.7.1 Telephone, VOIP, fax and video conference equipment 11

4.7.2 Data transmission and email 12

4.8 Manual Transmission 12

4.8.1 Within a single physical location 12

4.8.2 Transfer between establishments 13

4.8.3 Outside Australia 14

5 Glossary 15

6 Resources 16

Appendix A – Corporate File Cover and labels 17

Appendix B – Electronic document labelling 18

Appendix B (continued) 19
1 Introduction

Information is the basis upon which the Department conducts its business. As the custodians of a large amount of information that is either legally, personally, commercially or politically sensitive, the Department has a fundamental duty of care to ensure that the information we hold is secure. It is a responsibility that all employees share.

The Department expects its employees to protect departmental information against accidental or unauthorised modification, disclosure or loss.

2 Scope

These guidelines apply to all business centres of the NSW Department of Justice and all employees of the Department or any person or organisation who have access to or use of departmental information assets.

The following information assets are within scope of the guidelines:

- Information in all of its forms, whether printed or written on paper, stored electronically, transmitted by physical or using electronic means
- Information systems (e.g. hardware and software) used to process, control, transmit or store information in electronic format

These guidelines do not affect or alter existing legal and regulatory requirements under Commonwealth or NSW State legislation.

3 Purpose

This document provides detailed guidance on the protective handling measures of sensitive and security classified information.
The use of consistent and well-applied handling measures will enable staff to protect the integrity of vital records in respect of their movement, storage and handling in accordance with applicable legal and regulatory requirements.

4 Information Protection

4.1 Labelling

4.1.1 Interaction with Legislation

The presence or absence of a label/DLM/Protective marking will not affect a document’s status under governing legislation such as:

- Government Information (Public Access) (GIPA) Act 2009 NSW
- Privacy and Personal Information Protection Act (PPIPA) 1998 NSW
- Health Records and Information Privacy Act (HIPA) 2002 NSW

Where legislation, including that listed above, prevents the release or exchange of information, or encourages such release or exchange, regardless of how you have labelled it, the legislation will take precedence.

4.1.2 Unlabelled Information

Newly created or unlabelled material is by default UNCLASSIFIED and must be stored and handled according to NSW State Records standards and guidance and other NSW legislative and regulatory requirements as appropriate.

Material created on or after 1 July 2014 is regarded as unlabelled and UNCLASSIFIED where no protective marking is used.

4.1.3 Applying Protective Markings

Protective markings can be applied to information in any format, medium or resource including paper files or document, digital files or documents, information assets, datasets, infrastructure, records management systems, magnetic or optical media, microforms, databases, software applications, hardware and physical assets.

Apply markings when the information is created or received, or as soon as a high level of sensitivity becomes apparent.
4.1.4 Labelling Paper (hard copy) Documents

Sensitive and security classified documents should be filled with appropriate file covers. Refer to Appendix A for examples.

The relevant DLMs and security classification need to appear in:

- Capital letters,
- On the header and footer of each page, preferably be centred
- In red
- Arial 18, 5 mm in height

4.1.5 Labelling Electronic documents

The same labelling principle applies for electronic documents. The file security classification should be clearly visible whether it is paper or electronic. Refer to Appendix B for electronic document labelling examples.

4.2 Removal

Labels: UNCLASSIFIED FOUO, Sensitive, Sensitive:Personal, Sensitive:Legal

- 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.

Labels: UNCLASSIFIED Sensitive:NSW Government, Sensitive: Cabinet, Sensitive: NSW Cabinet

- 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

Removal from departmental premises only allowed when there is a definite need e.g. for use during meetings or short term work at home and where appropriate protection can be maintained en route and at the final destination
• Removal of protectively marked documents and material outside secure or authorised work area requires approval by the manager 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

• Protectively marked documents must be placed in a non-transparent envelope within a briefcase. The briefcase is to be locked at all times and under personal protection of the custodian. To prevent key duplication, keys should not be kept in the lock, even when the briefcase is empty and unlocked

• Electronic media such as laptops and portable hard disks that have been used to process protectively marked documents require the same protection as noted above

• If the security of information that is required for interstate meetings cannot be guaranteed by the person attending the meeting, it may be forwarded in advance by appropriate transfer arrangement (e.g. via authorised courier)

**Labels:** PROTECTED and CONFIDENTIAL

- Basis of real need, e.g., meeting
- Is to be in personal custody of individual and kept in a secure container (e.g. lockable briefcase, pouch, bag)
- Removal is to be authorised by the manager (or equivalent) responsible for the resource
- For home-based work, contact ITS Security for additional requirements

**Labels:** SECRET

- All the protections of PROTECTED and CONFIDENTIAL, and
- A written record of removal is to be maintained

**Labels:** TOP SECRET

- Contact ITS Security for detail requirements

4.3 Sharing

4.3.1 Receiving Commonwealth Information
NSW Department of Justice agencies must ensure that personnel who receive sensitive or security classified information are aware of their responsibilities and, where necessary, hold the appropriate security clearance.

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.

In the case where someone other than the intended addressee is charged with 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.

The recipient of a package containing security classified documents must verify that the information was transferred by the appropriate means and verify that its seals and packaging are still intact.

Agencies are to report any breakages, signs of tampering, or inappropriate methods of transfer to both the receiving and sending agency.

4.3.2 Information Shared with External Agencies or Third Parties

Where a Department of Justice agency needs to share sensitive or security classified information with external agencies, business partners or third party contractors, the following measures must be followed:

- Retain the security classification from originator
- Information asset must be managed in line with a Memorandum of Understanding (MOU), or Service Level Agreement (SLA) established between the agencies. It is the originating agencies responsibility to ensure that its information asset will be property protected
4.4 Copying

4.4.1 Approval from originator

Labels: UNCLASSIFIED (all DLMs)

Labels: PROTECTED, SENSITIVE and SECRET

Note: Copying Sensitive: NSW Cabinet document is always prohibited.

Copying protectively marked documents may be prohibited by originator. You must confirm whether such permission is granted prior to copying or printing. When seeking permission to make copies, the proposed additional distribution should be provided and the originator should indicate the appropriate copy numbers.

Labels: TOP SECRET (Please contact ITS Security for advice).

4.4.2 Spare copies

Labels: UNCLASSIFIED (all DLMs)

Labels: PROTECTED, SENSITIVE and SECRET

Copying information under these categories should be kept to a minimum with operational requirements and be performed only when necessary. Spare or spoiled copies should be destroyed immediately and in accordance with Section 4.6 Disposal in these guidelines.

Labels: TOP SECRET (Please contact ITS Security for advice).
4.4.3 Copy number

Labels: UNCLASSIFIED (all DLMs)

Labels: PROTECTED, SENSITIVE and SECRET

The originating agency’s permission is required before making copies of documents that have a copy number. It is preferable that any additional copies be provided by the originator.

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

Labels: TOP SECRET (Please contact ITS Security for advice).

4.4.4 Copiers, Printers and Multi-Function Devices (MFDs)

Labels: UNCLASSIFIED (all DLMs)

Labels: PROTECTED, SENSITIVE and SECRET

Copiers and printers should not be left unattended if information with protective markings or security classification is being reproduced unless there are suitable physical access controls to prevent unauthorised persons (including those without a need to know) from both entering the area around the copier or printer, and viewing the material being printed.

Individuals should stay within the immediate vicinity of the machine during copying or printing and remove reproduced protectively marked document immediately.

Multi-function devices may retain images of copied documents. Consult ITS Security for advice on data sanitisation of these devices.

Labels: TOP SECRET (Please contact ITS Security for advice).
4.5 Storage

4.5.1 Physical safe-keeping

Labels: UNCLASSIFIED (all DLMs)

Information with these protective markers must be secured when unattended and their contents must be unobservable to people without the need to know.

When not in use, hard copy and removable electronic media must be held in a commercial-grade locked container in a secure area.

Labels: PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET

Storage requirements for these classifications are determined by the security zone where information is located and the business impact of its compromise, loss of integrity or unavailability. Please contact ITS Security for advice.

4.5.2 Laptop and removable media

Labels: UNCLASSIFIED (all DLMs)

Sensitive information must be encrypted when stored in a laptop computer or on a removable hard drive, or storage device. Please contact ITS Security for advice.

Labels: PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET

The control requirements to store information under this security classification are determined by a security zone where information is located and its business impact level when compromise, loss of integrity or unavailability of that information occurs. Please contact ITS Security for advice.

4.6 Disposal

4.6.1 Paper items

Labels: UNCLASSIFIED (all DLMs)

- Do not dispose in a normal garbage or recycling paper bin
- Destroy using a cross cutting shredder, or
- Dispose in a locked secure bins
4.6.2 Other Media

Labels: UNCLASSIFIED (all DLMs)

- If media can be sanitised, use suitable degaussing tool to erase information. This should be performed using specifically designed security erasure software to effectively wipe the contents of media. Contact ITS Security for details.
- If media cannot be sanitised, it must be destroyed so that it cannot be recovered or reconstituted (e.g. disintegration using blades to cut, pulverisation using hammermills, burning etc)

Labels: PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET

Unless required for archival purposes, TOP SECRET material must be destroyed as soon as possible once it is no longer required for operational purposes.

The destruction method for media containing security classified information under this category depends on the media type. As a minimum requirement, it must be destroyed so that it cannot be recovered or reconstituted. Appropriate methods for each media item are defined by Commonwealth framework. Please contact ITS Security for advice.

4.7 Electronic Transmission

4.7.1 Telephone, VOIP, fax and video conference equipment

Labels: UNCLASSIFIED (all DLMs)
If transmission is:

- Infrequent (less than once a month) and unpredictable, or having low probability of interception, AND
- Over an agency’s private communication system within a single site, AND
- Using wire line or optic line (not wireless, cellular telephone or similar) then

It may be passed unencrypted without special controls.

If transmission is regular or frequent, agencies should conduct a risk assessment to determine whether encryption is appropriate for communications between sites or within sites using other than wire line or fibre optic transmission.

Labels: PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET (Please contact ITS Security for advice).

4.7.2 Data transmission and email

Labels: UNCLASSIFIED (all DLMs)

Infrequent or unpredictable transmission by email may be made without special controls over an agency’s private communications system.

Otherwise, an encryption based protection should be considered based on a risk assessment. Contact ITS Security for risk assessment and suitable encryption methods.

Labels: PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET (Please contact ITS Security for advice).

4.8 Manual Transmission

4.8.1 Within a single physical location

Labels: UNCLASSIFIED FOOU, Sensitive, Sensitive:Personal, Sensitive:Legal

A single sealed opaque envelope that indicates that the DLMs, delivered by the 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.
Labels: UNCLASSIFIED Sensitive: NSW Government, Sensitive: Cabinet, Sensitive: NSW Cabinet

A single sealed opaque envelope that indicates the DLM: receipt at the discretion of the originator AND:

- 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.

It may be passed, uncovered, by hand within a discreet 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.

Labels: PROTECTED

A single opaque envelope that indicates the classification, receipt at discretion of originator, and either;

- passed by hand between people who have the appropriate security clearance and ‘need to know’, or
- placed in a secure lockable briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger.

It 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.

4.8.2 Transfer between establishments

Labels: UNCLASSIFIED FOUO, Sensitive, Sensitive: Personal, Sensitive: Legal

A single sealed opaque envelope that does not indicate the sensitivity of the information; receipt at discretion of the originator AND one of the following;

- passed by hand between people who have the need to know
- delivered securely by an overnight courier that is endorsed in line with the agency security plan, or
• delivered by Australia Post, TOLL or a DX service.

Labels: UNCLASSIFIED Sensitive: NSW Government, Sensitive: Cabinet, Sensitive: NSW Cabinet

• A single sealed 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

• A double, sealed envelope AND receipt required AND delivered securely by an overnight courier that is endorsed in line with the agency security plan using the safe hand level of service.

Where personal or health information is being transferred, it is also necessary to comply with the requirements of PPIPA and HIPA respectively.

Labels: PROTECTED

Either

• A single opaque envelope that does not give any indication of the classification AND placed in a secure lockable briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger AND receipt required.

Or

• Double enveloping AND receipt required AND delivered either by approved overnight courier or by an agency specific alternative delivery services. Contact Records Management or ITS Security for approved delivery services.

4.8.3 Outside Australia

Labels: PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET

• Double enveloping required, receipt required and carriage by approved courier service or other authorised officers required. Contact Records Management or ITS Security for details.
## 5 Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable Material</td>
<td>In these Guidelines the term Accountable Material means particularly sensitive information requiring strict access and movement control. Such items are recorded in a central register in each holding organisation.</td>
</tr>
<tr>
<td>Central register</td>
<td>A central record is to be maintained of all persons having access to any information marked TOP SECRET or Accountable Material. This register is separate from any movement record which forms part of the document or file (see the PSPF for guidance).</td>
</tr>
<tr>
<td>Commonwealth</td>
<td>Refer to the Australian Government, and includes Australian Government agencies. Commonwealth does not include state government and its agencies.</td>
</tr>
<tr>
<td>Infrequent</td>
<td>The term Infrequent means no more than one transmission per month within or from a site.</td>
</tr>
<tr>
<td>Need to know</td>
<td>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. Agencies should take all reasonable and appropriate precautions to ensure that only people with a proven need to know gain access to sensitive and security classified information. People are not entitled to access information merely because it would be convenient for them to know or because of their status, position, rank or level of authorised access.</td>
</tr>
<tr>
<td>Unclassified</td>
<td>Official information that is not expected to cause harm and does not require a security classification; it may be unlabelled or it may be marked UNCLASSIFIED. UNCLASSIFIED is not a protective marking or a security classification. This type of information represents the bulk of official information.</td>
</tr>
<tr>
<td>PSPF</td>
<td>Australian Government Protective Security Policy Framework</td>
</tr>
<tr>
<td>PPIPA</td>
<td>Privacy and Personal Information Protection Act 1998 (NSW)</td>
</tr>
<tr>
<td>GIPA</td>
<td>Government Information (Public Access) Act 2009 NSW</td>
</tr>
<tr>
<td>DLM</td>
<td>Dissemination limiting marker</td>
</tr>
</tbody>
</table>
6 Resources

Following provides a list of key resources that may influence information security classification and handling procedures.

2. Information security management guidelines – Australian Government security classification system
3. Information security management guidelines – Australian Government - Protective marking and handling sensitive and security classified information
4. Physical security management guidelines – Australian Government – Security zones and risk mitigation control measures
5. Physical Security Management Guidelines – Australian Government – Physical security of ICT equipment, systems and facilities
6. Physical security management protocol – Australian Government
10. Australian Signals Directorate’s (ASD’s) Evaluated Products List (EPL)
11. NSW Digital Information Security Policy
12. Privacy and Personal Information Protection Act 1998 (NSW)
15. NSW Government Information Classification and Labelling Guidelines v1.1 October 2013
16. NSW Department of Justice Information Security Policy
17. NSW Department of Justice Records Management Policy
Appendix A – Corporate File Cover and labels

Corporate file cover (former Attorney General’s division)

File Labels example (CSNSW)
Appendix B – Electronic document labelling

Examples
CLASSIFICATION ONLY

DLM ONLY

BOTH CLASSIFICATION and DLM
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.
Appendix B (continued)

When using the DLM ‘Sensitive’

When applying a DLM of ‘Sensitive’ 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.

![Diagram showing cover page and first page with 'Sensitive' marking and relevant text.](image-url)
Appendix B (continued)

In this example the document contains more than one page, therefore the overall masking 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.

END OF DOCUMENT