Information Security Classification, Labelling & Handling Standard

Applicable to:
- Transport for NSW (TfNSW)
- NSW Trains
- State Transit Authority
- Sydney Trains
- Sydney Metro

The term “staff” is used in this Standard to cover all permanent, temporary or casual staff, staff seconded from another organisation. This procedure also applies to labour hire, professional, contractors and consultants engaged within the Transport Cluster. This Standard applies to any staff member who has or is given access to Transport cluster information assets, infrastructure, applications and/or services.

It applies to any record in any format (electronic, print or as a database) that may contain Transport cluster information.

Division: Corporate Services
Date of Publication 9 March 2020
Effective date: 9 March 2020
Review date: 9 March 2021
Document approver: Secretary
Document owner: Group CIO
Superseded documents: CPSt14001.3 Information Security Classification, Labelling & Handling Standard
Enquiries to: Email: infosec@transport.nsw.gov.au
## Contents

1 **Background** .................................................................................................................. 3
   1.1 About this document .................................................................................................. 3
   1.2 NSW Government policy framework ........................................................................ 3
   1.3 Related TfNSW Policies, Standards and Guidelines .................................................. 3
   1.4 Compliance ................................................................................................................. 3
   1.5 Exemptions .................................................................................................................. 3
   1.6 Key definitions .......................................................................................................... 4

2 **General Principles** ....................................................................................................... 4
   2.1 “Need-to-know” Principle ........................................................................................ 4
   2.2 Responsibilities .......................................................................................................... 4

3 **Information Classification and Labelling requirements** .............................................. 5
   3.1 UNCLASSIFIED material ......................................................................................... 5
   3.2 Dissemination Limiting Markers ............................................................................. 6
   3.3 Control and handling of security classified information ......................................... 6
   3.4 When to use caveats ................................................................................................. 7

4 **Information handling requirements** ........................................................................... 7
   4.1 General handling requirements ............................................................................... 7

5 **Media destruction and sanitisation** ........................................................................... 7
   5.1 Disposal and/or destruction ..................................................................................... 7
   5.2 Destruction and Sanitisation Standards .................................................................... 8
   5.3 Authority to destroy .................................................................................................. 8
   5.4 Documentation ......................................................................................................... 9

6 **Document History** ..................................................................................................... 10

7 **Attachments and Appendices** ................................................................................... 10
   7.1 Appendix A - Recommended Mapping to pre-2014 labels .................................... 11
1 Background

1.1 About this document

The objective of this Standard is to support the Transport Information Security Policy’s principle of empowering everyone with the responsibility for the appropriate protection of information owned by Transport or entrusted to it by a third party or the public.

This standard supports the Policy by defining the minimum standards required for information classification, labelling and handling across the Transport cluster.

1.2 NSW Government policy framework

The NSW Government’s Digital Information Security Policy requires all Transport cluster documents to be classified and labelled in accordance with the DFSI C2015-01 NSW Information Classification and Labelling Guidelines.

This Standard does not reproduce sections from NSW Government standards or guidelines and readers of this document are encouraged to read the source standard or guideline for detailed guidance; refer to section 7 Attachments and Appendices in this standard.

Guidance on translating pre-2014 classification labels for NSW to the new classification and labelling guidelines is noted in Appendix A - Recommended Mapping to pre-2014 labels.

1.3 Related TfNSW Policies, Standards and Guidelines

The Transport Information Security Policy and its supporting standards and guidelines are located on the TfNSW intranet. The Information Classification and Handling User Guide contains an FAQ and examples of use. Other guidelines and supporting documents may be found on the intranet.

1.4 Compliance

Staff must adhere to this Standard from 1 July 2015. Records classified and labelled prior to 1 July 2015 do not have to be re-classified and re-labelled until they are edited and reviewed for currency (in line with document management practices).

Where a contractual stipulation requires documents to be marked in a particular way, this Standard applies in addition to those contractual stipulations.

1.5 Exemptions

Non-compliance with this Standard may be conditionally approved for a maximum of twelve (12) months, with appropriate risk acceptance (based on TERM delegation of authority) and senior management endorsement of action plans. In addition to risk acceptance (based on a risk assessment undertaken by the requestor), grounds for consideration of an exemption are based on the following considerations:

- Technological obstruction or impossibility (in context of the agency business);
- Financially infeasible; and/or
- Agency business cannot operate without non-compliance.

Detailed supporting documentation addressing one or more of these criteria must be attached to the request which must be sought by using the process described in the TfNSW Exemptions Management Standard.
1.6 Key definitions
All terminology in this Standard is taken to mean the generally accepted or dictionary definition with the exception of the following terms which have a specifically defined meaning:

- **‘Should’ and ‘Should Not’** – non-compliance with ‘should’ and ‘should not’ statements are likely to represent a medium or low risk to an Agency. Therefore, Information Owners or Custodians can consider the justification for non-compliance and accept the associated risks.

- **‘Must’ and ‘Must Not’** - non-compliance with ‘must’ and ‘must not’ statements are likely to represent a high risk to Agency information and systems.

- **Staff**– all Transport cluster staff, as well as contractors and external parties who have access to Transport cluster information systems and Transport cluster information.

- **Manager** – Staff members that have a formal supervisory role for one or many staff member(s).

- **TfNSW** – the Transport for NSW organisation.

- **Transport** – All entities and Agencies that comprise the Transport Cluster.

2 General Principles

A label or marker identifies the protective procedures that must be provided during the use, storage, transmission, transfer and disposal of Transport cluster information.

All Transport cluster documents will be classified, labelled and handled in accordance with this Standard.

2.1 “Need-to-know” Principle

Staff must take all reasonable and appropriate precautions to ensure that only people with a demonstrated ‘need-to-know’ are able to access information. Staff members are not entitled to access information that is not required to undertake their tasks/job/role.

2.2 Responsibilities

**Staff** - are responsible for:

- classifying and labelling documents that they receive (if they do not have an existing classification), create or edit;

- being aware of their information security responsibilities;

- security of information under their control at all times (including when absent, by appropriately securing the information);

- maintaining compliance with this Standard at all times;

- taking precautions to ensure that security classified information is protected in line with this Standard, ensuring the risk of unauthorised access is minimised; and

- informing their Manager if they, or someone else, gains access to information that they are not authorised or security cleared to access.

**Managers** - are responsible for ensuring that:
• information within their area of responsibility is labelled and protected according to this Standard, and reviewed on a regular basis;
• Staff are provided with access to this Standard, and appropriately trained in the application of labelling and protecting information;
• Staff are assigned access to files and systems on a need-to-know basis aligned to their roles and responsibilities;
• requirements for access to security classified information are identified early, and arrangement for an appropriate Security Clearance is made with the Security and Emergency Management Branch; and
• Staff comply with this Standard.

3 Information Classification and Labelling requirements

According to the NSW Government Recordkeeping Manual Guidance in Brief 58, information classification is an important business issue and supports the maintenance of confidentiality, integrity and availability of information.

Most of the information within the Transport cluster is expected to be UNCLASSIFIED and only marked with a Dissemination Limiting Marker (DLM) if required.

DLMs are markings for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling, see 3.2 Dissemination Limiting Markers for more information.

The NSW Government has also developed a simple interactive web tool that allows users to click through a series of questions to determine whether a DLM is required. The app can be accessed at http://finance.nsw.gov.au/ict/app/.

3.1 UNCLASSIFIED material

UNCLASSIFIED information requires only limited protection. This information should be marked bold text and a minimum of 5mm high (preferably red stamp).

• Arial Font – at least size 12 (e.g. UNCLASSIFIED);
• Times New Roman – at least size 14 (e.g. UNCLASSIFIED).

UNCLASSIFIED is not a security classification. UNCLASSIFIED is used to describe information that is not expected to cause harm and does not require a security classification.

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

As stated in DFSI C2015-01 NSW Information Classification and Labelling Guidelines:

• records created on or after 1 January 2014 are regarded as UNCLASSIFIED where no protective marking has been used; and
• information labelled or classified before 1 July 2015 does not need to be re-labelled or re-classified unless specifically required due to a business or operational need.

The presence or absence of a protective marking will not, by itself, affect a document’s status under relevant NSW Acts or Regulatory requirements (e.g. Government Information
3.2 Dissemination Limiting Markers

DLMs are markings for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling.

The NSW Government has also developed a simple interactive web tool that allows users to click through a series of questions to determine whether a DLM is required. The app can be accessed at http://finance.nsw.gov.au/ict/app/.

There are three categories of protective markings:

1. dissemination limiting markers
2. security classifications, and
3. caveats.

Specific definition of each protective marking is set out in DFSI C2015-01 NSW Information Classification and Labelling Guidelines section 4, 5 and 6 respectively.

Information that does not meet the criteria for security classification but which requires some lower level of protection can be labelled with a DLM.

The Australian Government system includes five DLMs:

1. For Official Use Only (FOUO)
2. Sensitive
3. Sensitive: Personal
4. Sensitive: Legal, and
5. Sensitive: Cabinet

In NSW, four additional DLMs are used:

1. Sensitive: NSW Government
2. Sensitive: NSW Cabinet
3. Sensitive :Law Enforcement
4. Sensitive: Health Information

Transport cluster information may be marked with any of the DLMs noted in DFSI C2015-01 NSW Information Classification and Labelling Guidelines.

3.3 Control and handling of security classified information

A security clearance is required for handling security classified information. Security clearances and reviews of a person’s background and suitability to access security classified information are required for those few positions in the Transport cluster. All security clearance requests within the Transport cluster are to go via the Security and Emergency Management Branch.

Access to security classified information is predicated on having the relevant level of security clearance, and having an established need-to-know. There are specific storage, handling and destruction requirements defined in DFSI C2015-01 NSW Information Classification and Labelling Guidelines (Section 5). For guidance on the control and handling of security classified information, agencies should refer to the DFSI C2015-01 NSW Information Classification and Labelling Guidelines (Section 5), PSPF and the guidance provided in the Information Security Management Guidelines - Protectively Marking And Handling Sensitive And Security Classified Information.
Note: Transport cluster staff will only have a limited need to access security classified information at PROTECTED and above. This reflects our business and the fact that most records can be managed using a DLM. TfNSW Information & Communications Technology (ICT) systems are currently not accredited to handle, store or transmit security classified information.

3.4 When to use caveats

Certain security classified information, most notably some national security classified information, may bear a security caveat in addition to a security classification. The caveat is a warning that the information has special requirements in addition to those indicated by the protective marking. Caveats are not used with DLMs and caveats are not used on their own without an accompanying security classification. Caveats should not be used extensively in NSW.

People who need-to-know will be cleared and briefed about the significance of information bearing caveats; other people are not to have access to this information.

For guidance on the use of caveats, agencies should refer to the DFSI C2015-01 NSW Information Classification and Labelling Guidelines (Section 6), PSPF and the guidance provided in the Information Security Management Guidelines - Protectively marking and handling sensitive and security classified information.

4 Information handling requirements

4.1 General handling requirements

Information must be used and shared according to its sensitivity and business needs. Information may be shared internally or with third parties and DFSI C2015-01 NSW Information Classification and Labelling Guidelines Appendix E provides detailed guidelines for the protection of information with various classification and/or markings.

All TfNSW documents will be handled in accordance with this Standard.

5 Media destruction and sanitisation

All Transport cluster documents, devices and media containing Transport Information will be sanitised and/or destroyed in accordance with this Standard. Media containing Transport cluster documents includes paper, electronic storage, CD/DVD, USB and flash drives and memory cards, amongst others.

5.1 Disposal and/or destruction

Information and records may only be destroyed in accordance with the Transport Records Disposal Procedure. The Information Owner must assess risk and establish strategies to protect information and records during the media destruction and sanitisation process.

A factor influencing a sanitisation or destruction decision is who has control and access to the media. This aspect must be considered when media leaves Transport cluster control. Media control may be transferred when media are:

- returned to an external entity at the end of a leasing agreement; or
- being donated or resold to be reused outside the Transport cluster; or
- being replaced due to fault or upgrade; or
• being thrown away due to fault or any other reason.

Media leaving Transport cluster control must be sanitised or destroyed unless the purpose of the media leaving Transport cluster control is for the recovery of Transport cluster information from the media. Information and records must be protected during this process. Devices or media that will be reused within the Transport Cluster may require sanitisation based on the classification of the information stored or managed.

Examples of “under Transport cluster control” and “not under Transport cluster control” control are listed below.

5.1.1 Under Transport cluster control

• Media turned over for maintenance to a third-party if contractual agreements are in place between TfNSW and the maintenance provider that specifically provides for the confidentiality of the information;
• Maintenance on media performed on a Transport cluster site, under TfNSW supervision, by a TfNSW-authorised maintenance provider; and
• Media relocated to another Transport cluster site or archive.

5.1.2 Not under Transport cluster control

• Media exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to Transport cluster;
• BYO devices that are enrolled and trusted that belong to a person leaving Transport cluster employment or leaving a Transport cluster engagement;
• BYO devices that are enrolled and trusted that are sent for repair outside a Transport cluster site;
• Any physical electronic or electromagnetic media (operable or not) where the intention is to dispose of it; and
• Traditional media (paper, microfiche etc.) sent for recycling or any other purpose other than relocation to another Transport cluster site or archive.

5.2 Destruction and Sanitisation Standards

The Information Owner must ascertain information classification of the media and, using the following ISM documents, decide on a suitable method of destruction or sanitisation. Subject to information classification, media sanitisation is permitted by any of the methods defined in the ISM Controls, Media Security, and Media Sanitisation and ISM Guidelines Protectively Marking and Handling Sensitive and Security Classified Information, s10. Media sanitisation must comply with the principles for destruction outlined in the Transport Records Disposal Procedure.

5.3 Authority to destroy

The Transport Records Disposal Procedure is applicable to all Transport agencies. This Procedure defines the authorisation process for disposal and provides detail on where there is no requirement for authorisation.
5.3.1 Backup media and TfNSW service providers
Service providers to TfNSW must obtain approval from TfNSW SecOPS for the destruction of backup tapes or disposal of other media that has contained TfNSW information. If the media being destroyed is backup media, the request to TfNSW must specify that the media are TfNSW backup media and supply a reason for media destruction.

5.4 Documentation
Before the media are destroyed or sanitised, the Information Owner must ensure that risk of information loss has been assessed and that a strategy has been put in place to ensure that information and records are protected. The agency must produce a list that contains:

- details of media, including a unique identifier;
- method of destruction or sanitisation;
- name of service provider;
- if applicable, location of disposal after sanitisation; and
- reasons for destruction or sanitisation.

The documentation must also include the method of transporting media from storage to the destruction site. The transportation should have sufficient physical security to prevent unauthorised access.

5.4.1 Destruction certificate
The destruction service providers (internal to TfNSW or third-party) must provide a destruction certificate. The certificate should contain at least the dates and method of destruction, unique identifying information for each item destroyed, and, where possible, the location of destroyed material.

5.4.2 Disposal certificate
A service provider or agency must provide a list of media that have been sanitised for reuse. If the re-use is outside the Transport cluster (by sale, auction or any other method), then the certificate must contain the dates and method of sanitisation, unique identifying information for each item sanitised, disposal method of sanitised material and, where possible, the location of disposed sanitised material.

5.4.3 Audit authority
Transport agencies are responsible for establishing an audit and monitoring framework to ensure that unauthorised disposal of records and information does not take place. Additionally, TfNSW has the authority to audit destruction, disposal and/or sanitisation of any media and may apply suitable methods to ascertain that the provisions of this standard have been followed.
6 Document History

<table>
<thead>
<tr>
<th>Date &amp; PD No</th>
<th>Approved by</th>
<th>Amendment Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014 CP14001</td>
<td>ED HRBS</td>
<td>Replaces SS04 Security Standard – Information Security Classification and Labelling to comply with new Policy and Standards templates, and updates to NSW Government Information Classification and Labelling Guidelines</td>
</tr>
<tr>
<td>CPS14001.1 9 December 2016</td>
<td>Secretary</td>
<td>Replaces SS-06: Secure Destruction Updated to reflect DFSI C2015-01 NSW Information Classification and Labelling Guidelines</td>
</tr>
<tr>
<td>1 July 2018 CPS14001.2</td>
<td>Secretary</td>
<td>Inclusion of Sydney Metro as agency to which this policy applies from 1 July 2018.</td>
</tr>
<tr>
<td>15 August 2019 CPS14001.3</td>
<td>Secretary</td>
<td>Updates to obsolete position titles, Division name and template changes to front page.</td>
</tr>
<tr>
<td>9 March 2020 CPS14001.4</td>
<td>Secretary</td>
<td>Removal of RMS as an Agency to which this Policy applies (update to front page).</td>
</tr>
</tbody>
</table>

7 Attachments and Appendices

The following documents can be found on the internet:

1. DFSI C2015-01 NSW Information Classification and Labelling Guidelines  

2. NSW Government Digital Information Security Policy  


4. Transport Records Disposal Procedure Australian Government security classification system  

5. NSW Government Recordkeeping In Brief 58  

6. Transport Records Disposal Procedure  
### 7.1 Appendix A - Recommended Mapping to pre-2014 labels

<table>
<thead>
<tr>
<th>Business Impact Levels</th>
<th>Previous NSW label</th>
<th>Dissemination Limiting Marker (DLM) Listed in order of most to least likely.</th>
<th>Security classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Impact</td>
<td></td>
<td></td>
<td>UNCLASSIFIED</td>
</tr>
<tr>
<td>Low to Medium</td>
<td>PERSONNEL-IN-CONFIDENCE</td>
<td>Sensitive: Personal</td>
<td>UNCLASSIFIED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sensitive: NSW Government</td>
<td></td>
</tr>
<tr>
<td>Low to Medium</td>
<td>COMMERCIAL-IN-CONFIDENCE</td>
<td>Sensitive: NSW Government</td>
<td>UNCLASSIFIED</td>
</tr>
<tr>
<td>Low to Medium</td>
<td>CLIENT-IN-CONFIDENCE</td>
<td>Sensitive: Personal</td>
<td>UNCLASSIFIED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sensitive: NSW Government</td>
<td></td>
</tr>
<tr>
<td>Low to Medium</td>
<td>SECURITY-IN-CONFIDENCE</td>
<td>Sensitive: NSW Government</td>
<td>UNCLASSIFIED</td>
</tr>
<tr>
<td>Low to Medium</td>
<td>STAFF-IN-CONFIDENCE</td>
<td>Sensitive: Personal</td>
<td>UNCLASSIFIED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sensitive: NSW Government</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>CABINET-IN-CONFIDENCE</td>
<td>Sensitive: NSW Cabinet</td>
<td>PROTECTED</td>
</tr>
<tr>
<td>High</td>
<td>PROTECTED</td>
<td>Sensitive: NSW Government</td>
<td>PROTECTED</td>
</tr>
<tr>
<td>High or Very High</td>
<td>HIGHLY PROTECTED</td>
<td>Sensitive: NSW Government</td>
<td>PROTECTED CONFIDENTIAL SECRET</td>
</tr>
<tr>
<td>Extreme</td>
<td></td>
<td></td>
<td>SECRET</td>
</tr>
<tr>
<td>Catastrophic</td>
<td></td>
<td></td>
<td>TOP SECRET</td>
</tr>
</tbody>
</table>