NSW Government Information Classification, Labelling and Handling Guidelines

Document number: 2.0	Date: 06 August 2020

Contact details

Business Unit: Data.NSW, Data Analytics Centre	Division: Customer, Delivery and Transformation
Email: datansw@customerservice.nsw.gov.au	

Table of Contents

1. Overview

1.1 Purpose

The NSW Government sector receive, use and manage information and data[1] on behalf of the NSW public, other agencies, states and territories and the Australian Government[2]. This information is important and often sensitive. It is important that this information is labelled correctly so that the users of it within NSW Government know how to manage it in an appropriate, secure and careful way that is consistent with the Australian Government, and other states and territories.

The NSW Government Information Classification, Labelling and Handling Guidelines (Guidelines) align with the Australian Government's *Protective Security Policy Framework* (PSPF) 2018, focusing on; Policy 8 *Sensitive and security classified information* and the *Email Protective Marking Standard*. Policy 9 *Access to information*, Policy 15 *Physical security for entity resources* and Policy 11 *Robust ICT systems* have also informed these Guidelines.

Aligning the Guidelines with the PSPF will enable information to be more readily shared among NSW Government agencies and the Australian Government.

The Guidelines detail how the NSW Government sector can correctly assess the sensitivity or security classification of their information and adopt labelling, handling, storage and disposal arrangements to protect information.

The Guidelines have been developed to enable agencies;

- to understand how to assess NSW Government information and data to determine if:
    - the information is OFFICIAL or UNOFFICIAL
    - the information is sensitive and the reason for the sensitivity
    - a security classification must be applied.
- to understand the labelling of information and data received from the Australian Government and how to handle this information in accordance to the label.
- Once the security classification or sensitivity of the information has been assessed, these Guidelines describe how the information should be labelled, handled and disseminated.

[1] Throughout this document we use 'information' to denote 'information and data'.
[2] Throughout the document, Australian government is used to refer to the Commonwealth of Australia

1.2 Audience

These Guidelines apply to the NSW Government sector, which includes all Public Service Agencies (for a full definition, see the *Government Sector Employment Act 2013)*. The term 'Agency' is used in these Guidelines to refer to all NSW Government sector agencies.

The Guidelines are intended for use by agency staff in roles that involve:

- receiving, creating or editing information
- developing systems to collect, manage and store information (e.g. developers)
- administering information and controlling user access
- protecting information from misuse or access by unauthorised users.

The Guidelines are recommended for adoption in state owned corporations, as well as local councils and universities.

1.3 Scope

The Guidelines apply to the classification, labelling and handling of sensitive and security classified information in any format, including records in physical and digital format, data sets and digital records.

Agencies must refer to the relevant requirements in the PSPF for classifying and handling security classified information under the PSPF, i.e. PROTECTED, SECRET and TOP SECRET – particularly in relation to information affecting national security as this forms part of the memorandum of understanding (MoU) for the Protection of National Security Information.

The MoU has been agreed to by Commonwealth, and states and territories of Australia. This MoU is under review and the proposed new changes are minor, updating references to the PSPF instead of to the superseded Australian Government Protective Security Manual (PSM).

The MoU states that national security information be treated in a manner consistent with the minimum requirements set out in the PSPF (previously the PSM). The MoU provides the framework for:

- A nationally consistent approach to the protection of national security information, including the management of national security clearances; and
- All jurisdictions to put in place policies and arrangements appropriate to their circumstances for the protection of national security information.

This MOU is not legally binding and is a statement of mutual intent and understanding.

The Guidelines do not affect or alter existing legal and regulatory requirements under Australian Government or NSW Government legislation, including under the *Government Information (Public Access) Act 2009 (NSW)* (GIPA), the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIPA), the *Health Records and Information Privacy Act 2002 (NSW)* (HRIPA) and the *State Records Act 1998 (NSW)*. Existing privacy principles applicable under NSW Government and/or Commonwealth legislation continue to apply to the handling of information.

Where an agency engages a contractor or third-party provider, the agency is responsible for ensuring the contractor or third-party provider complies with the Guidelines.

1.4 Superseded NSW guidance

These Guidelines supersede the NSW Government Information Classification, Labelling and Handling Guidelines (2015).

1.5 Summary

This document supersedes the 2015 NSW Government Information Classification, Labelling and Handling Guidelines. It incorporates the Australian Government's PSPF, first published in 2018.

These Guidelines are aimed at helping agencies understand how to correctly assess the sensitivity or security classifications of information they hold, how to label this information and how to manage this information according to the label.

The Guidelines align with the PSPF. Existing Dissemination Limiting Markers (DLMs) have been continued from the 2015 Guidelines at the request of NSW agencies, with minor variations.

Compromise, either deliberate or accidental, of sensitive or security classified information could result in harm to an individual, organisation or government. Applying labels (protective markings) to sensitive or security classified information indicates that the information requires protecting and dictates the level of care needed. Protective markings are an easily recognisable way for information users and systems to identify the level of protection the information requires.

The key aspects of the Guidelines are as follows:

- UNOFFICIAL information is not work related.
- OFFICIAL information is related to the agency's business but does not have security or sensitivity issues. This information does not need to be labelled but agencies may choose to do so. This information is still important to government and may still need security measure to protect the integrity and availability of this material.
- Sensitive information, if compromised, may cause limited damage to individuals, organisations or government. The Australian government uses one DLM (OFFICIAL: Sensitive). NSW uses six DLMs to describe the type of sensitivity of the information.
    1. OFFICIAL: Sensitive – NSW Cabinet
    2. OFFICIAL: Sensitive – Legal
    3. OFFICIAL: Sensitive – Law enforcement
    4. OFFICIAL: Sensitive – Health information
    5. OFFICIAL: Sensitive – Personal
    6. OFFICIAL: Sensitive – NSW Government.
- These DLMs can also be used with security classifications.
- There are three security classifications under the PSPF:
    1. PROTECTED

2. SECRET

3. TOP SECRET.

- A set of minimum handling guidelines have been created for sensitive information for NSW.
- A separate set of handling guidelines for security classified information from the PSPF have been included
- Information is assessed using the business impact levels tool.

1.6 Agency-specific policies and procedures

Agency-specific policies and procedures for classification, labelling and handling should identify:

- who is responsible for information classification and labelling
- who is responsible for the policies and procedures governing the alteration of protective markings
- what information requires classification, labelling and handling
- who would be using the protectively marked information
- any unique procedures for handling that information and complying with legislation
- how to communicate the requirements and responsibilities for handling protectively marked information within and external to the agency
- if the agency can handle security classified information on digital systems
- when individuals should consult with their security team for advice on the application of protections for sensitive and security classified information. Agencies may need to implement the protections in particular ways or to apply a higher level of protection, in order to meet business needs or to address the entity's security risk environment.

Agencies must determine specific events or dates for de-classification based on the duration of the information's sensitivity, and regularly review the level of protective marking applied to information. This must be done in accordance with an agency's internal policy and procedures.

In developing internal policies and procedures, agencies must apply principles of good information security practices:

- information should be open by default but protected where required[3]
- sensitive information should only be released to organisations and individuals who demonstrate a need-to-know
- information is to be stored and processed away from public access
- information can only be removed from agency for an identified need
- disposal of information is by secure means
- information transmission and transfer are by means which deter unauthorised access.

***Need-to-know** principle applies for all access to sensitive and security classified information. Limiting access by staff and others (e.g. contractors) to information on a need-to-know basis guards against the risk of unauthorised access or misuse of information. Staff 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. Having a security clearance does not automatically give the right to know.*

Internal agency procedures should outline any standard processes for protectively marked material, including:

- creation and storage
- dissemination and use
- archiving and disposal.

[3] In accordance with the NSW Government Open Data Policy

2. Assessing information for its security classification and sensitivity

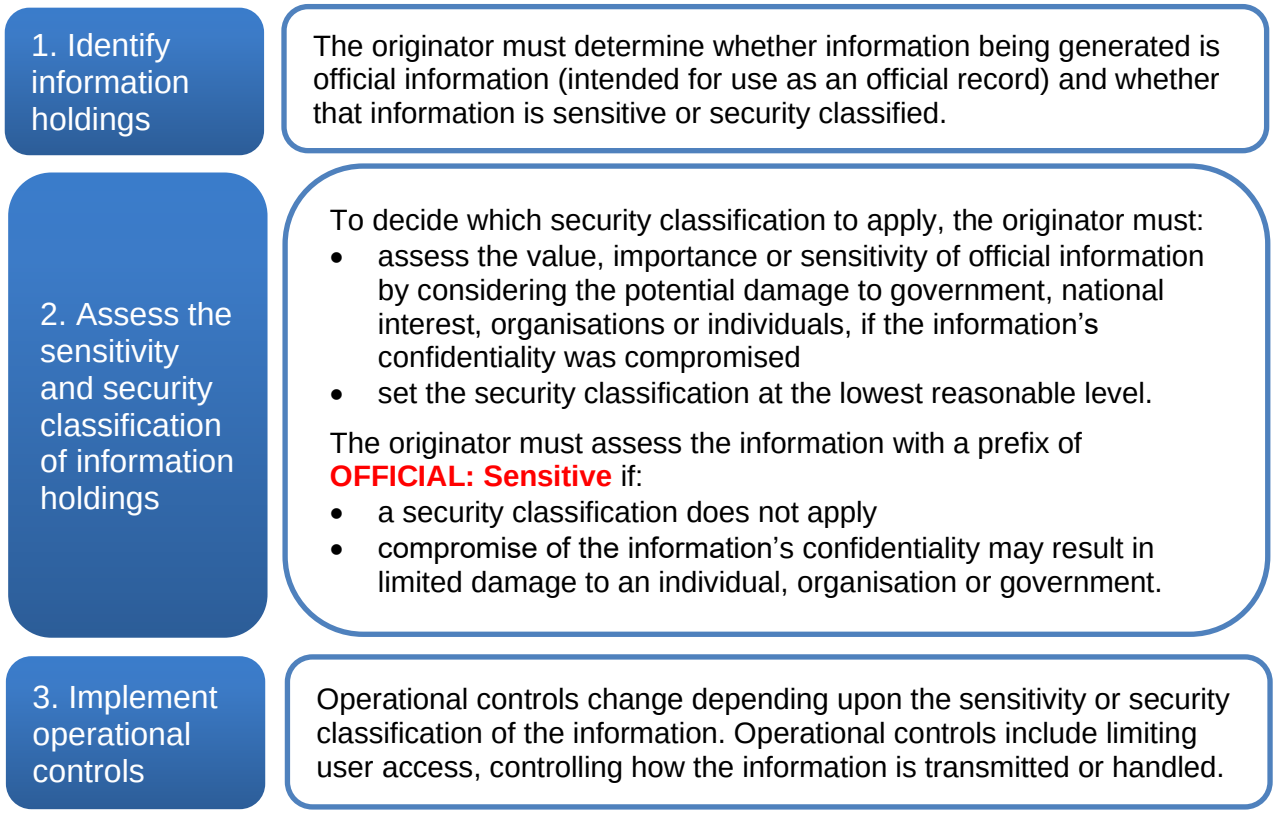
Information is a valuable resource. Protecting the confidentiality, integrity and availability of information is critical to business operations.

- **Confidentiality** of information refers to limiting access to information to authorised persons for approved purposes.
- **Integrity** of information refers to the assurance that information is authentic, correct and valid and can be trusted.
- **Availability** of information refers to allowing authorised persons to access information for authorised purposes at the time they need to do so.

The person or agency responsible for generating, preparing or actioning information is called the originator.

Each agency must identify information holdings, for example their customer relationship management programs, assess the sensitivity and security classification of information, and implement operational controls for these information holdings proportional to their value, importance and sensitivity (see Figure 1).

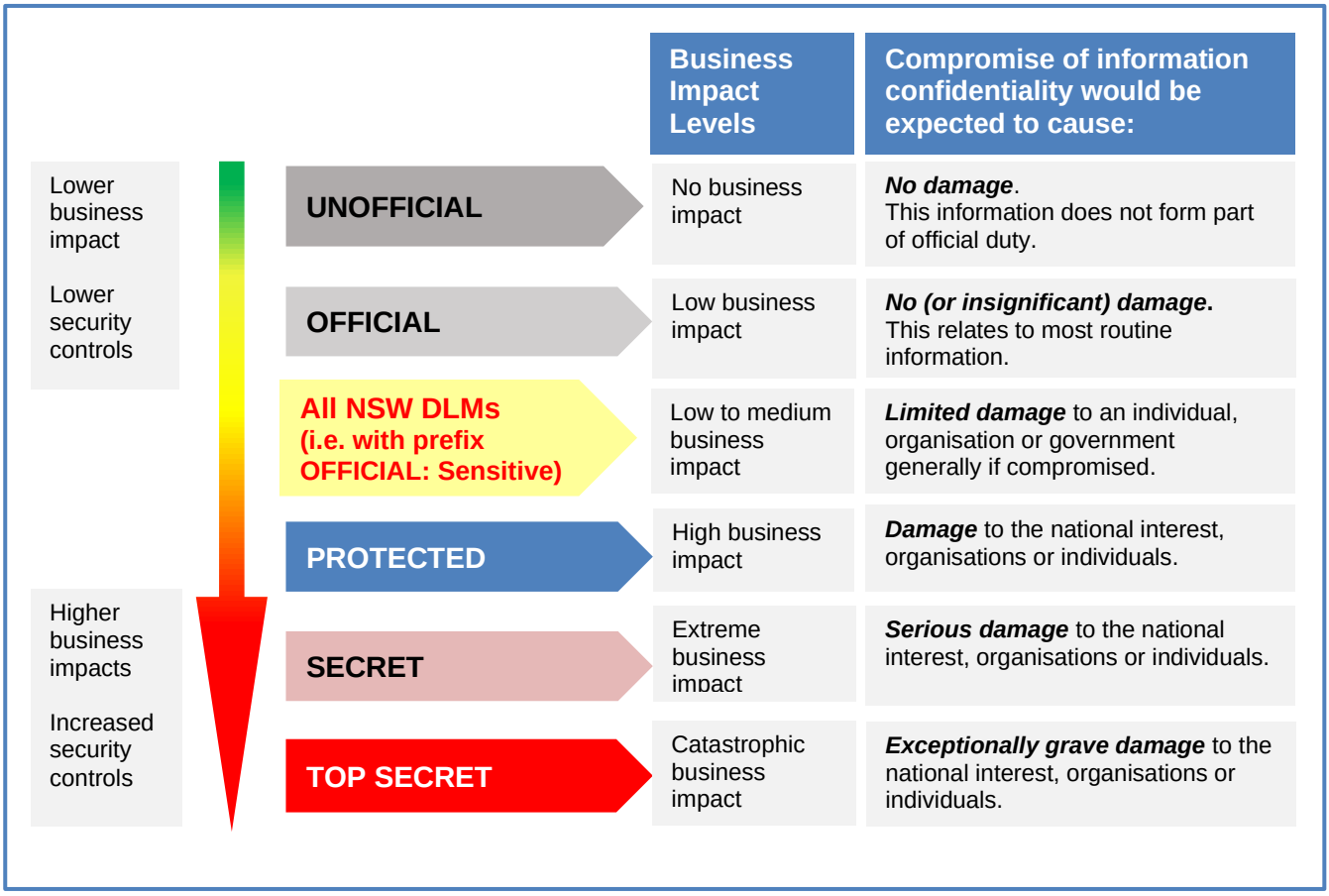
Figure 1: Three step process to identify, assess and implement protective controls



2.1 Assessing sensitivity and security classified information

As the importance of the information increases, so does the level of control – from few controls for UNOFFICIAL information to very tight controls for TOP SECRET information. The level of damage caused by a compromise of the information confidentiality also increases, as shown in Figure 2.

Figure 2: Using business impact levels (BIL) to assess sensitive and security classified information



2.2 Over-classification

NSW Government agencies are expected to use a DLM or security classification **only** when there is a clear and justifiable need to do so.

Over-classification can have a range of undesirable outcomes, including:

- unnecessary limitation of public access to information
- unnecessary imposition of extra administrative arrangements and additional cost
- excessively large volumes of protected information, which is harder for an agency to protect
- devaluing protective markings so that they are ignored or avoided by staff, contractors or receiving agencies.

2.3 Using the business impact levels tool

The business impact levels (BIL) tool provides parameters to assess potential damage from compromise of the confidentiality of information. The tool assists in the consistent classification of information and the assessment of impacts on government business.

This tool considers potential impact on the:

- individual
- organisation
- legal compliance
- compiled data
- government
- Australian economy
- infrastructure
- international relations
- crime prevention, defence or intelligence operations.

The business impact levels tool must be used to assess information for its sensitivity or security classification.

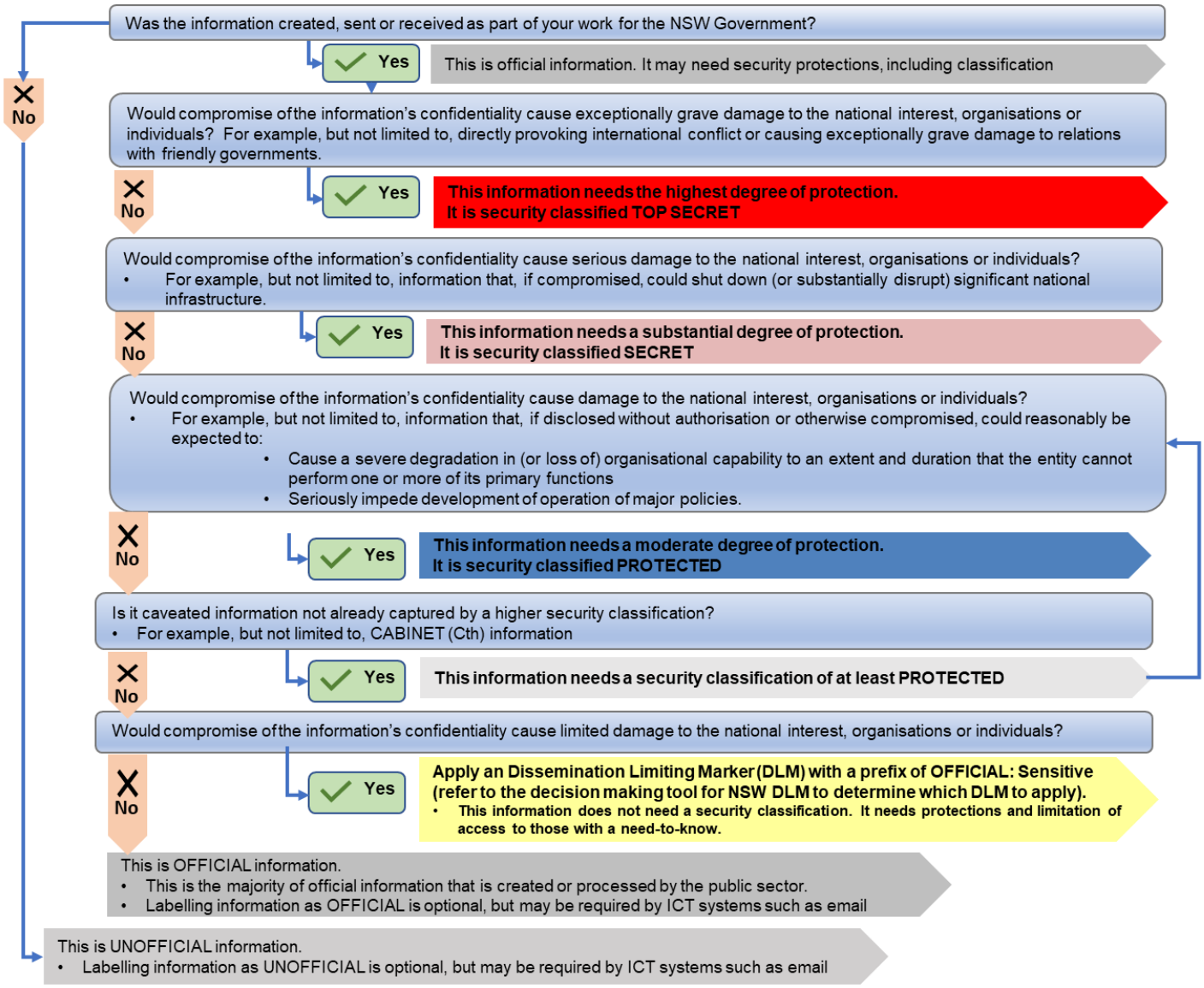
The BIL tool has been modified slightly for use in NSW and can be found in Appendix 1. When assessing information using the tool **all sub impact categories need to be used** to make the assessment, and then the security classification should be set at the **lowest reasonable level**.

The intent of the BIL tool is to provide a way of consistently assessing potential damage due to compromise of information, however the classifications also need to be practically applied. Limiting the dissemination of information due to security classification could also have a negative impact if the people who need to know are unable to view the information when they require it. A pragmatic and risk-based approach is recommended.

***Example**: An agency has sensitive information within a dataset and is trying to decide if it should be labelled with a NSW DLM or a security classification of PROTECTED, using the BIL tool. Considering the assets and finances sub-impact category, if the unauthorised release of information could cause* limited damage *to an agency's asset or operational budget estimated to be between $10 million to $100 million dollars, the information would be labelled with a NSW DLM with a prefix of OFFICIAL: Sensitive. If the unauthorised release could cause* damage *between $100 million to $10 billion, then the information would be labelled as PROTECTED.*

Often it is the difference between assessing information as sensitive (requiring a DLM) or assessing the information as PROTECTED which causes the most concern for NSW agencies. Figure 3 describes a way to help determine if a document is sensitive or if a security classification is needed.

[4]Figure 3: Assessing whether information is sensitive, or security classified



[4] Caveated information is described in chapter 7.

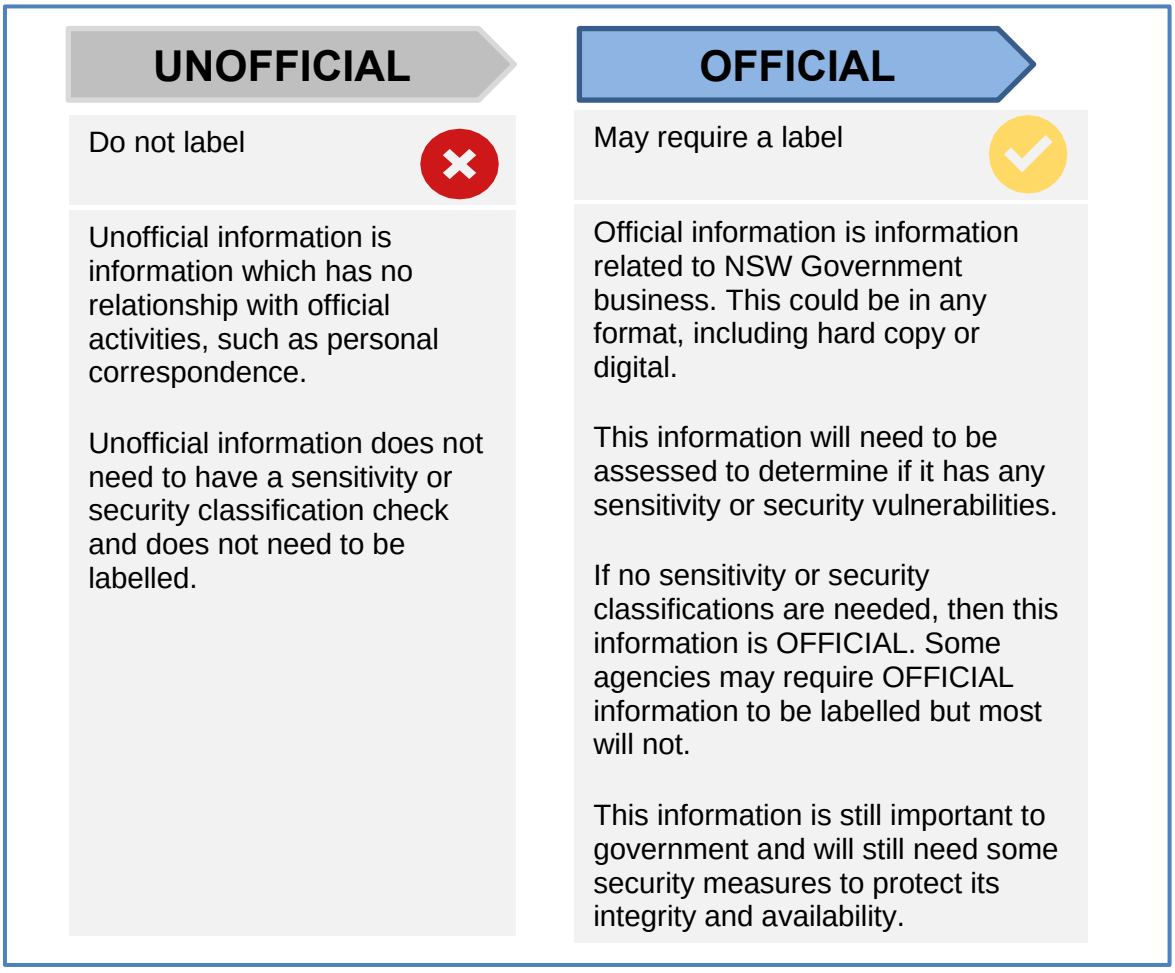
3. Labelling different types of information

3.1 Unofficial or official information

Official information is all information created, sent or received as part of the agency's work. This information is an official record and provides evidence of what an agency has done and why. UNOFFICIAL information is information which does not relate to the agency's work, such as a personal email. OFFICIAL information has been assessed as relating to the agency and does not have a sensitive or security classification. See Figure 3 for an illustration of the key differences.

Previously, information handled by the NSW Government which had a low sensitivity could have been marked as UNCLASSIFIED. This label has been replaced by the OFFICIAL label.

Figure 3: Unofficial and official information may not need to be labelled



Agencies must implement operational controls to protect information in proportion to their value, importance and sensitivity. Although these guidelines are focused on sensitive and security classified information, all official information requires an appropriate degree of protection as information (and assets holding information) are subject to both intentional and accidental threats. In addition, related processes, systems, networks and people have inherent vulnerabilities. A deliberate or accidental threat that compromises information security could have an adverse impact on government business.

4. Sensitive information

The NSW Government collects, stores and manages sensitive information as a part of normal business processes. Sensitive information includes:

- personal information
- health information
- information which could be subject to legal privilege
- commercial-in-confidence information
- law enforcement information
- NSW Cabinet information

Examples of sensitive information are an individual's personal details, credit information, medical records, drivers licence information, criminal records, biometric information and other personal details.

Compromise of this information's confidentiality may result in *limited damage* to an individual, organisation or government generally and requires additional care in handling. It could result in fraudulent use of an individual's personal information, financial loss to the agency or the individuals affected or the reputational damage and loss of public trust in the agency responsible for the safekeeping of the information.

Collection, storage, use and disposal of different types of sensitive information is governed by different legislation and requires different access and dissemination rules. To make these differences clear, NSW Government uses dissemination limiting markers (DLMs) that must be applied to sensitive information. Most DLMs can be used on their own, or in conjunction with a security classification.

Dissemination limiting markers (DLMs) are labels used by the NSW Government to define sensitive information and data, both physical and digital.

4.1 Labelling sensitive information

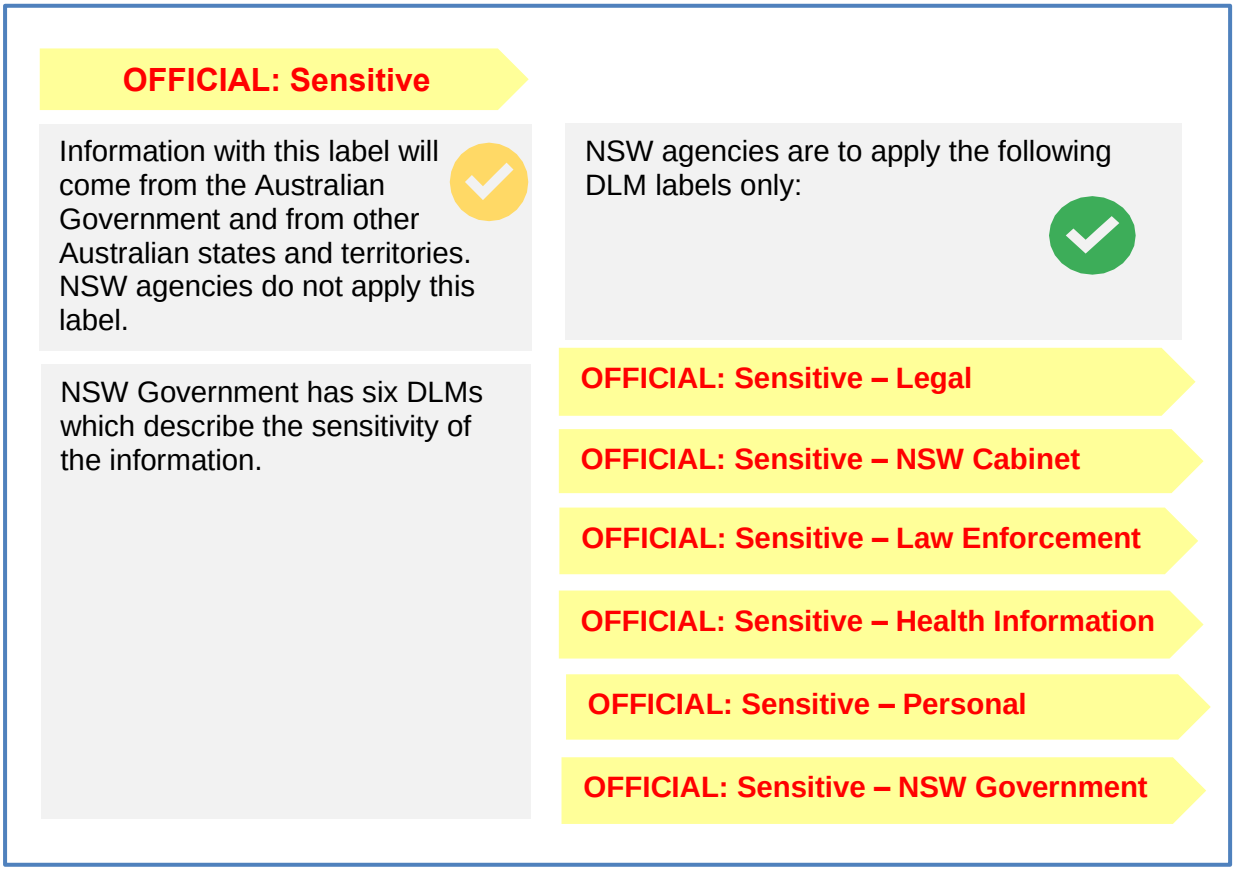
In NSW, sensitive information must be labelled with a DLM. This label helps the user of the information understand why the information is sensitive and what the limitations on dissemination are.

The Australian Government uses the OFFICIAL: Sensitive label for information which, if compromised, would cause *limited damage* to the national interest, organisations or individuals. This information is not security classified but it does need protection and limitation of access to those who need to know.

NSW Government legislation differs to other states and the Commonwealth. To easily understand and identify information dissemination limitations relevant to different legislation, NSW uses six labels.

The OFFICIAL: Sensitive label will be applied by the Australian Government, and other states and territories. The NSW Government will not apply this label to its information because the six DLMs used in NSW with the OFFICIAL: Sensitive prefix allow for the specificity required in NSW. This means that information labelled OFFICIAL: Sensitive will be deemed to have originated from outside of NSW Government. See Figure 4 for a summary.

Figure 4: Official sensitive information with DLMs



Applying a text-based DLM labels with a prefix of OFFICIAL: Sensitive to documents (including emails).

It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For NSW DLMs a yellow colour is recommended. If text or colour-based protective markings cannot be used, apply the agency's marking scheme.

If marking paragraphs abbreviations can be used. The Australian Government DLM OFFICIAL: Sensitive can be abbreviated to (O:S).

Hard copy and electronic records:

The label on a file cover or container must be at least equal to the label on the most sensitive item with the file or container. Labels need to be shown on all types of documents, reports and media.

Electronic and other documents should include their sensitivity label in their metadata.

Digital and data:

Sensitivity and security labelling of digital information should be applied and communicated to the users of the systems. Sensitivity labelling can be shown in metadata fields within programs, in data dictionaries and system documentation.

Some systems may not have the functionality to include sensitivity or security classification labelling. In this case, an induction or communication program should be run with staff using the system, including third party users, to ensure they understand the sensitivity of the information they have access to.

Table 2 describes how to apply the NSW DLMs and the legislation which underpins each label.

Table 2: Applying NSW DLMs

Label	When to apply the label	Legislation or policy underpinning the label
OFFICIAL: Sensitive (This is an Australian Government DLM)	The Australian Government and other Australian states and territories may send information with this label. NSW agencies should **not** re-label information received from the Australian Government and other Australian states or territories. This label is not applied to NSW information. NSW Government will label information with NSW DLMs as described below.	Protective Security Policy Framework
OFFICIAL: Sensitive - NSW Cabinet	Label all NSW Cabinet documents with **OFFICIAL: Sensitive – NSW Cabinet.** Confidentiality of cabinet documents, including draft cabinet documents, is maintained to enable full and frank discussions to be had prior to cabinet making its decision. The NSW Department of Premier and Cabinet maintains a secure electronic document management system which is the repository for all official records of the NSW Cabinet. This system has its own access and handling guidelines.	Cabinet Conventions: NSW Practice Government Information (Public Access) Act 2009 - Schedule 1 contains information about overriding secrecy laws which apply to NSW cabinet information.
OFFICIAL: Sensitive – Personal	Apply this label to information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This includes an individual's fingerprints, retina prints, body samples or genetic characteristics.	Privacy and Personal Information Protection Act 1998 No 133
OFFICIAL: Sensitive – Health Information	This label should be used for health-related information. Under the HRIP Act, this means personal information that is identifying information, or which could reasonably link to identifying information, collected from or about individual people in order to provide them with health services.	Health Records and Information Privacy Act 2002 No 71 NSW Health Privacy Manual for Health Information Health Records and Information Privacy Regulation 2017

Label	When to apply the label	Legislation or policy underpinning the label
OFFICIAL: Sensitive – Legal	Use this label for any information subject to legal professional privilege. The Evidence Act refers to confidential communication and documents: *Confidential communication* means a communication made in such circumstances that, when it was made: (a) the person who made it, or (b) the person to whom it was made, was under an express or implied obligation not to disclose its contents, whether or not the obligation arises under law. *Confidential document* means a document prepared in such circumstances that, when it was prepared: (a) the person who prepared it, or (b) the person for whom it was prepared, was under an express or implied obligation not to disclose its contents, whether or not the obligation arises under law.	Legal Profession Uniform Law (NSW) No 16a Legal Profession Uniform Law Application Act 2014 No 16 Evidence Act 1995 No 25
OFFICIAL: Sensitive – NSW Government	Use this label if the compromise of this information will cause limited damage to an individual, organisation or government in general. For example, where compromise could; • endanger individuals and/or private entities • lead to financial loss to the agency or the individual • cause reputational damage and loss of public trust in the agency.	
OFFICIAL: Sensitive – Law Enforcement	This label should be applied by law enforcement agencies, investigative agencies and agencies with legislated compliance and enforcement responsibilities. For further details about this DLM refer to section 4.2 of the Guidelines.	Law Enforcement (Powers and Responsibilities) Act 2002 No 103 There are many pieces of legislation in NSW which contain additional legislative restrictions to the provision of access to information through secrecy clauses, dissemination limiting clauses for law enforcement or investigative purposes. Use this label for these.

4.2 OFFICIAL: Sensitive – Law Enforcement DLM

The purpose of the OFFICIAL: Sensitive – Law Enforcement DLM is to enable law enforcement agencies, investigative agencies and agencies with legislated compliance and enforcement responsibilities, to more easily understand the information they are handling, to enable sharing of information between agencies and to have common handling procedures.

The presence or absence of a DLM will not affect a document's status under existing legislation. The guidelines do not affect or alter existing legal and regulatory requirements under Australian Government or NSW legislation.

OFFICIAL: Sensitive – Law Enforcement DLM should only be used by law enforcement agencies, investigative agencies or agencies with legislated compliance and enforcement responsibilities, for law enforcement purposes and for information that needs to remain strictly confidential.

Information compiled for law enforcement purposes is often complex and may contain personal, health and law enforcement activity information. This information is important and should be afforded appropriate security in order to protect enforcement proceedings, the right of a person to a fair trial, policing and community safety practices, proprietary information or to protect a confidential source.

Information with a NSW DLM of **OFFICIAL Sensitive – Law Enforcement** which is provided to another agency for law enforcement purposes is not to be released by that agency to a third party without the written approval of the law enforcement agency that created the information. This includes information sought through various freedom of information legislation or court subpoenas. It is best practice for agencies who use this label on documents (physical or digital), to include information about which agency the information originates from.

The information that may fall under these activities includes:

- multi-jurisdictional operational law enforcement activity
- policies and guidelines for law enforcement investigations when disclosure of could be reasonably expected to risk circumvention of the law, or jeopardise the life or physical security of any individual, including the lives and safety of law enforcement personnel
- law enforcement training information.

The use and dissemination of law enforcement information is strictly regulated, and it may constitute a criminal offence to use or release it for any purpose that is not authorised by

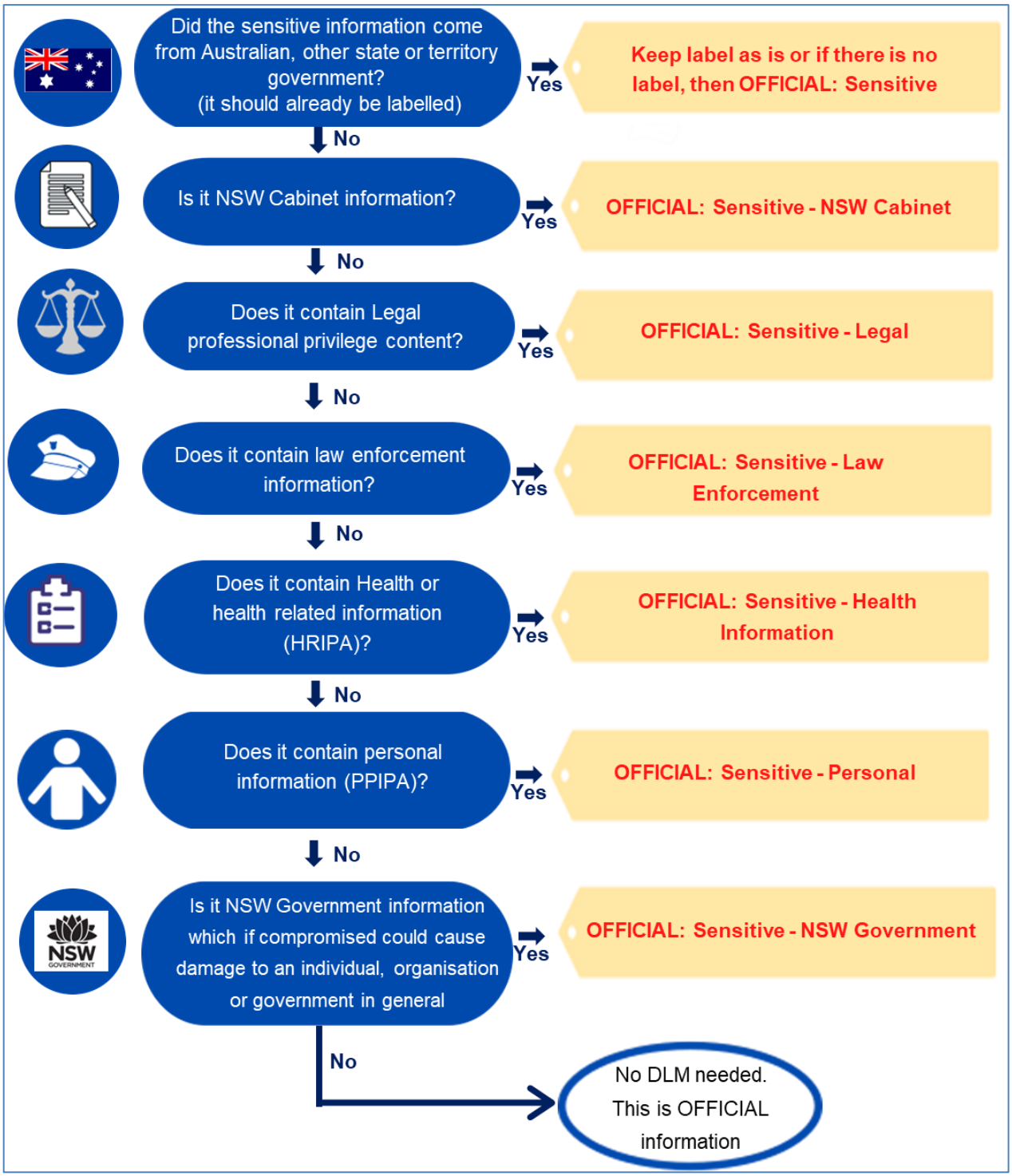
the acts. Where personal or health information is being transferred as part of a law enforcement operation, it is also necessary to comply with the requirements of the appropriate state privacy legislation.

OFFICIAL: Sensitive – Legal and **OFFICIAL Sensitive – Law Enforcement** DLMs should not be confused. **OFFICIAL: Sensitive – Legal** should be used to protect legal professional privilege under the advice of legal professionals.

4.3 Determining which OFFICIAL: Sensitive NSW DLM to apply

Figure 5 outlines a simple decision-making process that NSW Government agencies can use to determine which NSW DLM can be applied to information of a sensitive nature.

Figure 5: Decision making tool for NSW DLMs



4.4 Why do I have to label?

Applying labels (protective markings) to security classified or sensitive information indicates that the information requires protection and dictates the level of protection required. Protective markings help control and prevent compromise of information as they are an easily recognisable way for information users (visually) and systems (such as an entity's email gateway) to identify the level of protection the information requires. The labels describe why the dissemination of the information is limited.

4.5 Creating new DLMs

Agencies are not to create their own DLMs, security classifications or caveats.

4.6 What if my information falls under two labels?

Two labels are not required, the decision-making tool (Figure 5) has been designed to help determine which label to use. Most health information contains information about health as well as personal information and this should be labelled as **OFFICIAL: Sensitive - Health Information**.

In a situation where a document has multiple types of information, or information that fits more than one DLM or security classification, the document must be labelled and/or classified as per the information of the highest level of sensitivity within that document.

4.7 Who applies the label?

The person responsible for preparing the information is responsible for assessing the information and labelling it according to these guidelines.

NSW agencies are likely to manage sensitive information that has historically not been labelled. Sensitive information in use must be labelled. NSW agencies need to plan how to implement labelling across their organisation based on risk and importance of the information; for example, more sensitive or confidential information should be labelled first.

Agencies are to advise all staff, including contractors, on the proper use of the information classification, labelling and handling guidelines. Agencies that are likely to handle sensitive information should have standard operating procedures to assist staff in labelling.

4.8 When are the labels applied?

Labels should be applied when:

- the information is created. The originator is required to assess the consequences or damage from unauthorised compromise or misuse of the information. If adverse consequences from compromise of confidentiality could occur or the agency is legally required to protect the information, the information must be labelled.

- information is received from external sources, that is not already labelled, should be assessed upon receipt and labelled according to its sensitivity or security requirements. Security classified information which is received from another government agency should be handled in accordance with these guidelines and the Protective Security Policy Framework (PSPF) as appropriate. Re-labelling of information received from another government agency is not necessary unless information has been added, edited or removed and its sensitivity or security classification has changed. This re-labelling should be done in consultation with that agency.

The label **For Official Use Only** *is no longer used.*

Agencies are not required to label UNOFFICIAL or OFFICIAL information. By default, unlabelled information will be handled as OFFICIAL. Agencies may determine their own policy for labelling OFFICIAL material, according to their operating requirements.

A NSW agency sending sensitive information to another government agency must label the information with a DLM so that the receiving agency will understand the sensitivity of the information.

The originator must ensure that information is classified and labelled prior to any use or sharing of the information. Information custodians are to provide appropriate classification and handling guidance to any third-party requiring access to the information.

If you receive a document or record that is already labelled, the document or record needs to be handled according to this label. Re-labelling of documents is not required unless it is obvious that the document contains sensitive or confidential information that may be at risk of exposure. If a decision to re-label is made, contact the originator of the information, if possible, to inform them of the need to amend the label.

4.9 Where should the label be applied?

Once you have assessed the information and determined that it needs a DLM, you now need to apply these labels to the information. DLMs can be applied to information in any format and medium. This includes paper or digital.

The labels need to be at the top and bottom centre of the documents, presentations, maps, media, so they are visually prominent. Examples have been provided below.

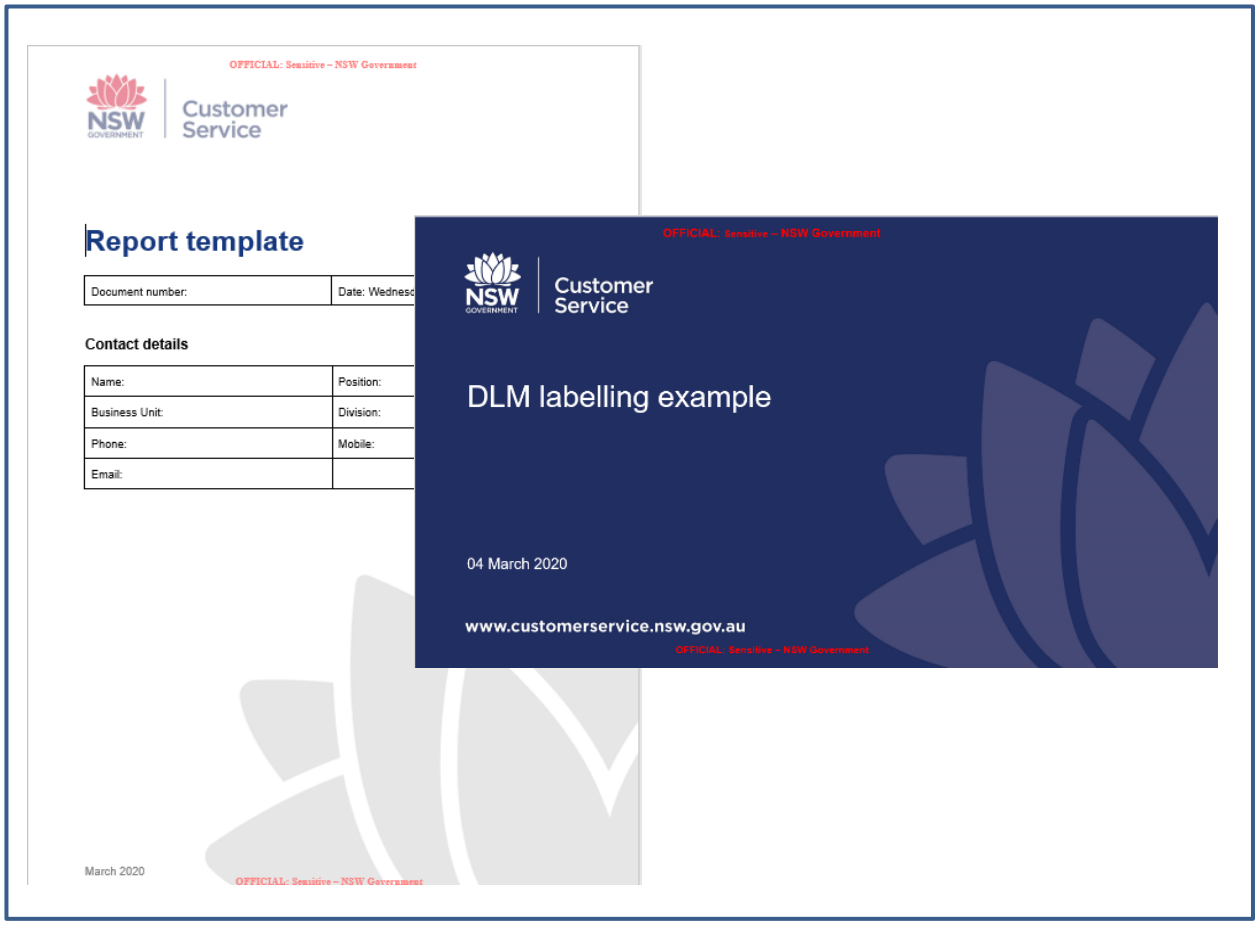
4.9.1 Email – agencies with Microsoft 365 may decide to set up automatic labelling of emails. Emails need to be marked in the subject line as well as at the top and bottom of the message. Email labelling is required for sensitive information and above even if automatic labelling has not been implemented.

Figure 6: Example email with labels in the subject line and at the top and bottom of the email.

The Australian Government has developed an email protective marking standard for Australian government agencies to follow. This standard has been applied to the example in Figure 6 which is why the email subject line looks a little different to the header and footer of the document.

4.9.2 Documents – agencies are to insert a label in the header and footer of each document.

Figure 7: Example documents labelled in the header and footer.



4.9.1 Metadata – Sensitivity and security classifications should be included in the metadata about digital records or data; this ensures that the information about the sensitivity and security classifications are obvious, and persistent. Labelling can be applied at field level using metadata depending upon the application. Sensitivity and security classified labels should be added to data catalogues.

4.10 I think the label is wrong – what do I do?

The originator of the information is responsible for labelling the document and changing these labels. If the document appears to be labelled incorrectly the originator needs to be contacted and the information re-labelled. If the originator is not known, the information needs to be assessed using the business impact levels tool and labelled accordingly.

4.11 What if the information's sensitivity changes over time?

Sensitivity of information can change over time and will need to be reassessed and labelled accordingly, particularly digital records and datasets. Agency datasets which are populated by free text fields through internet applications need to be monitored frequently and labelled according to the type of information provided.

Salesforce is a system used by the Department of Customer Service to manage customer records. This database is developing over time as new projects are added. The sensitivity and confidentially of this information may change, therefore needing periodical review, label and metadata change.

The originator and data custodian must monitor information sensitivity over time. Associated dynamic information products, data analytics and third-party applications will also need to update the labels if changed.

Sensitivity of information can change over time for example a document may be sensitive until it is published but not afterwards.

4.12 Do I have to update the existing labels in my agency?

These labelling guidelines are not retrospective. If information is not being used, the original labels can be kept. If the information is in use, it is expected that this information will be relabelled with new labels. A risk management approach should be taken with this process, with the higher risk or more sensitive information being relabelled first.

4.13 Receiving Australian Government information

The Commonwealth requires that NSW Government agencies receiving Australian Government sensitive and security classified information comply with the procedures set out in the PSPF regarding the application, removal, transfer, receipt and destruction of that information. Refer to PSPF Policy 8 Sensitive and security classified information for more information.

PSPF Policy 9 Access to information establishes the level of security clearance required to access sensitive and security classified information. Further guidance on obtaining personnel security clearances see PSPF Policy 12 Eligibility and suitability of personnel and your agency's Security Clearance Officer.

It is the responsibility of the information sender to ensure that security classified documents are protected appropriately. Recipient agencies are responsible for determining their obligations to protect the information according to the confidentiality requirements of the protective markings.

5. Handling sensitive information

5.1 What does handling of sensitive information mean?

Handling means the way in which information is managed, how the information is accessed, stored, transferred or transmitted, shared, archived and disposed of. Sensitive information is important as it could contain personal or health information and if compromised, could cause limited damage to government, organisations or individuals. As a result, a higher level of controls to protect and manage this information is required.

A minimum set of handling guidelines for sensitive information has been developed to enable greater consistency between NSW agencies in the way in which information is understood and handled, while still allowing some flexibility for agency specific differences in systems and processes.

Security clearances are required for authorisation for ongoing access to PROTECTED, SECRET and TOP SECRET information but are not required for handling NSW DLM information with a prefix of OFFICIAL: Sensitive.

5.2 Minimum handling requirements for NSW DLMs

A set of minimum handling requirements for sensitive information applies to DLMs. Each NSW DLM describes a different category of information sensitivity and each refers to different NSW Government legislation. The legislation drives the purpose of the information collection, how this information should be managed and who can and cannot access this information.

Whether intentional or unintentional, unauthorised disclosure of OFFICIAL: Sensitive information can have serious consequences. All agency staff are employed under a code of conduct which imposes obligations of confidentiality.

All sensitive information is important, and a set of minimum handling requirements are set out below:

Collecting

- Collect information only for a lawful purpose that is reasonably necessary, and directly related to a function or activity of the agency. Collection methods, including online surveys, must have secure storage.
- Label digital information that is collected. This includes information captured via automated processes, for example via batch processes or API. This information should be labelled in metadata if the system allows and/or via system documentation ideally at the time the system is developed.

Labelling

- Label sensitive or security classified information at the time of collection or creation. Labelling is not retrospective, if information is not in use, there is no need to re-label with new labels. Information in use should be re-labelled. Agencies with large volumes of information with out-of-date labels should re-label information according to its risk profile.
- If receiving information that is already labelled, do not re-label. If there are questions about the validity of the label consult the data originator.
- Labelling of entire systems and large datasets needs to be carefully considered as this could restrict access to information unnecessarily. Labelling at field, case or record level may be more appropriate if the system has the capability. Access to field, case or records with higher sensitivity within a system or large dataset can be managed via user access permissions, only giving access to users that need-to-know.

Monitoring

- Monitor information over time to determine if the sensitivity of the information has changed. Change the label and security classification if required.
- Keep access audit logs for the appropriate retention period to assist in future audit and access control monitoring. Protect these logs from accidental or deliberate modification.

Storing

- Store hard-copy records and information in a designated location, in lockable storage or secure access areas. Store digital records, information and data in your agency's designated corporate recordkeeping systems or business systems. For more specific guidance check your agency's internal policies and legislation relevant to your work.
- Maintain inactive sensitive data to reduce risk of loss or theft. The risk of exposure of sensitive data increases when applications are retired or migrated, or SharePoint sites and file shares are abandoned at the conclusion of a project. For specific guidance about migration or retiring applications, check with your agency's information management team.

Accessing

- ✓ Apply the need-to-know principle to all information labelled with a NSW DLM and to any security classified information.
- ✓ Access to information labelled with a NSW DLM should be restricted. The information (or data) custodian at each agency has overall accountability for access provided (to hard copy, digital records, information and data).
- ✓ Ensure access to information labelled with a NSW DLM is only provided for a clear and legitimate business reason.
- ✓ Manage user access on an ongoing basis as roles and personnel change. The need for ongoing access or a time limited period of access should be considered.
- ✓ Review access to information systems containing information labelled with a NSW DLM by directly linked 3rd party applications. Information made available to these 3rd party applications must be limited to need-to-know. User access of the 3rd party applications need to be controlled as does the level of information that the users of this application can view. Examples of third-party applications are business and data analytics programs.
- ✗ Access rights cannot be transferred. Usernames and passwords should be kept confidential and not shared.
- ✗ Security clearances are not required for access to information labelled with a NSW DLM.

Securing

- ✓ Agencies must assess all data transiting and at rest and make an assessment whether it should be encrypted.
- ✓ Protect assets which contain sensitive information such as laptops or mobile devices.
- ✓ Secure mobile devices after use in a lockable container within agency facilities and if possible, outside of agency facilities, for example if working from home.
- ✗ Do not use your device unless it is safe to do so. Be aware of your surroundings. When sensitive and security classified information is being used, that can be read, viewed, heard or comprehended, it may be at a higher risk of compromise. Different physical environments pose different risks for information compromise.

Using

- ✓ Lock your computer screen or log out of secure systems when you leave your desk and make sure hard copies are secure (clear desk and clear screen policies should be implemented).
- ✓ Train all staff using sensitive information or using a secure system, so they are aware of the nature of the sensitive information and the rules which apply to use the information. Rules include whether they can view, print, share, or email information.
- ✓ Manual transfer of information labelled with a NSW DLM may be passed by hand within a discrete office environment provided it is transferred directly between members of staff who need-to-know and there is no opportunity for any unauthorised person to view the information.
- ✓ When carrying physical information labelled with a NSW DLM outside an agency facility, this information is to be carried in an opaque envelope or folder.
- ✗ Do not access information labelled with a NSW DLM using public networks.
- ✗ It is best practice to not copy information labelled with a NSW DLM onto local drives nor removable mobile storage devices such as USBs. Check your agency's internal policies.
- ? Follow your agency security measures if accessing information labelled with a NSW DLM outside an agency facility such as from home, via mobile devices. Where appropriate, ensure multifactor authentication is enabled and use only approved agency VPNs. For more specific guidance check your agency's internal policies and legislation relevant to your work. An example of this is your agency's work from home policy.
- ? When travelling outside Australia with mobile devices that can access, store or communicate information labelled with a NSW DLM, seek permission from your agency. Circular C2016-4 outlines the NSW Government policy for overseas travel.
- ? Copying, faxing, scanning, photographing and printing of information labelled with a NSW DLM should only be carried out if permitted by your agency and then only on a printer or device that has controlled access. For more specific guidance check your agency's internal policies and legislation relevant to your work.

Using - *Reports, Dashboards, Products*

Handle system generated reports, dashboard and products with legacy marking of “Sensitive” as per these guidelines and update labels when able, based on risk assessment. For example, the most sensitive or most viewed reports should have their labels updated first. Labelling is not retrospective.

Do not display products such as reports or dashboards containing sensitive information unless the audience need-to-know, and permission has been sought from the data custodian.

Sharing

If sharing data externally, reducing the sensitivity of the information by de-identification techniques is recommended, for example removing personal information or information revealing law enforcement procedure. The DLMs indicate why the information is sensitive and which legislation may be limiting the use of the information.

If sharing information externally, it is preferable that the source information is redacted to conceal the sensitive information where possible. This ensures that the source information remains inviolate and that the information can be safely shared. Care must be taken that the redaction does not alter the source information.

Agencies will each have their own policies about emailing sensitive information internally and externally. Best practice when emailing sensitive information from one agency to another agency, or from one location to another within an agency, should be done via secure file transfer protocol, or via a secure system that is recommended by your agency. Sensitive information should not be stored in emails or as attachments to email in your inbox. Email systems are at higher risk of compromise than approved corporate business systems and are at risk of accidental forwarding. For more specific guidance check your agency’s internal policies and legislation relevant to your work.

Share information labelled with a NSW DLM for authorised purposes only. Agencies must establish their own rules on how their sensitive information is to be disseminated and what the approval process is. In some cases, agencies require written approval before information can be shared. Other agencies can share information if there is a memorandum of understanding in place. Legislation also has dissemination limiting clauses. For more specific guidance check your agency’s internal policies and legislation relevant to your work.

Archiving, Retention and Disposal

Records, information and data are covered by the requirements of the *State Records Act 1998*. Procedures for disposal and archiving are agency specific. Sensitive information must be disposed of securely. For more specific guidance check your agency’s internal policies and legislation relevant to your work.

5.3 Can I email sensitive information?

Although each agency has its own email policies which apply to emails sent internally, to other agencies and externally, **best practices** are outlined below.

Emails should be labelled to show that the information contained within the email, or attachments to emails, contain sensitive information. Some NSW agencies have implemented cloud-based enterprise productivity solutions, which have the capability to select sensitivity and security classification in the subject line, header and footer of emails as well as other programs such as word processing or spreadsheet applications.

Emailing sensitive information between agencies may be permitted. Many agencies have memoranda of understanding (MOUs) in place to make sure that information can be shared in a safe way. Increasingly, interagency applications are being used to transfer information more securely, as user access to information can be controlled and monitored. The risk of accidental forwarding of information is also reduced. If you are emailing between agencies, please check your own agencies policies. MOUs do not negate legislative requirements. Check relevant legislation before sending or sharing information to make sure there are no secrecy or dissemination limiting clauses.

Secure information management systems such as eCabinet, used by the Department of Premier and Cabinet will have their own rules about emailing documents from these systems.

Emailing sensitive information is not generally recommended and encryption is recommended if transferred over public network or though unsecured spaces, unless the residual security risk of not doing so has been recognised and accepted by the agency.

A more secure method of transferring sensitive information is via a secure file transfer facility or a secure system that is recommended by your agency. Sensitive information received via email should not be stored in the email system or on local drives. Email communication can pose a higher risk of information compromise because of the ease of on-sharing the information and unauthorised access to email systems.

5.4 Can I print sensitive information?

Sensitive information should generally not be printed unless unavoidable or systems are in place to protect the confidentiality of the information.

Secure information management systems will have their own guidelines. For example, the eCabinet system records which documents are printed and these are required to be returned to the NSW Department of Premier and Cabinet, before being marked off and destroyed.

5.5 How do I destroy sensitive information?

Agencies must retain records and information in accordance with the *State Records Act 1998* (NSW) and any other legal and accountability requirements. Agencies should refer to applicable Functional Retention and Disposal Authorities and General Retention and Disposal Authorities for further information on the retention and disposal of records and

information. See NSW State Archives and Records' destruction of records for advice on the secure and confidential destruction of sensitive records and information. For advice on transferring records required for the State Archives collection, see transferring records guidance. Agencies should contact their internal records management staff or NSW State Archives and Records at govrec@records.nsw.gov.au if they have any queries about the retention and disposal of records and information.

All NSW agencies must ensure that records relating to child sexual abuse that has occurred or is alleged to have occurred be retained for at least 45 years as per the Royal Commission into institutional responses to child sexual abuse (2017) Volume 8, Recordkeeping and information sharing.

5.6 How do I handle compiled data?

A compilation of information (referred to in the PSPF as aggregated data) may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications.

Agencies will need to manage and retain compiled data in accordance with the *State Records Act 1998* (NSW) and any other legal and accountability requirements.

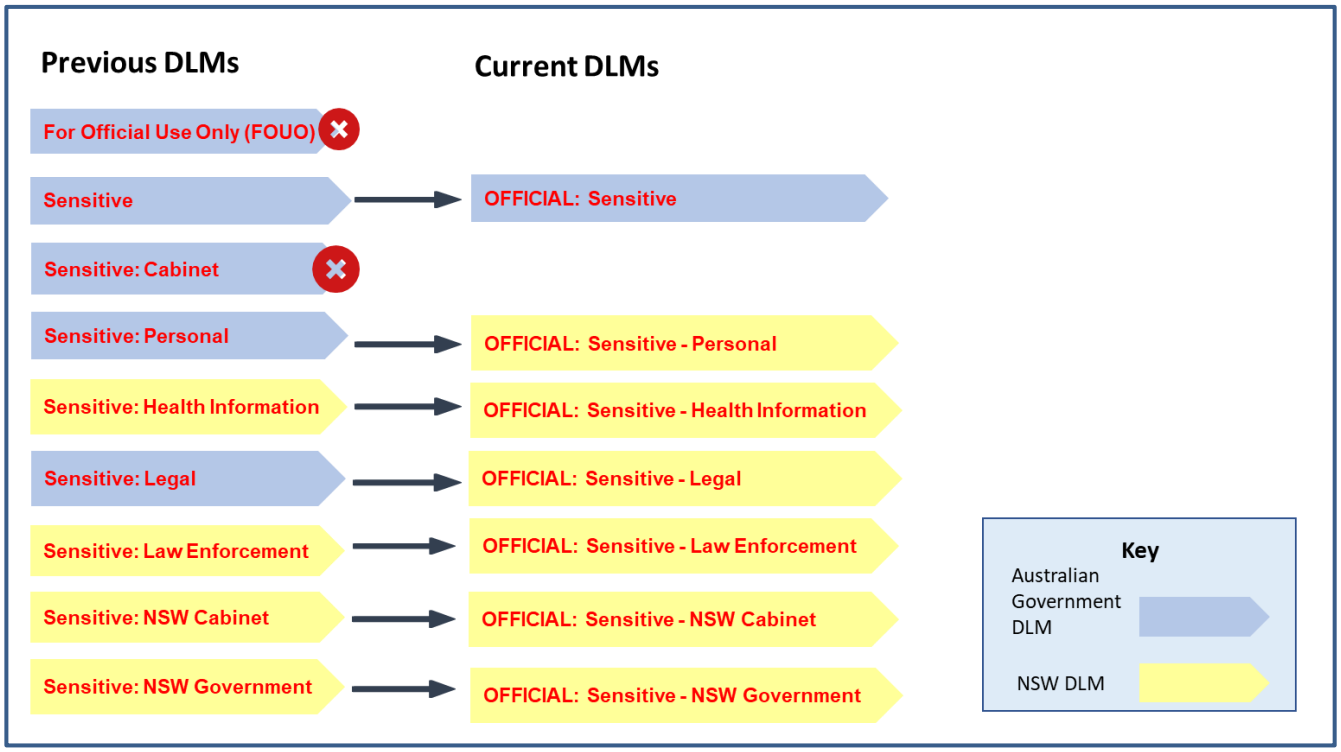
5.7 How do I handle automated transfer of sensitive data?

All access to sensitive data is on a need-to-know basis. If access has been granted, sensitive data which can be transferred automatically for example via integration software program, direct system links or applications, must to be labelled so that the users of the information understand the sensitivity and do not accidently compromise the confidentiality of this information.

5.8 Mapping old DLMs to new DLMs

Figure 8 shows the previous and current DLMs. The DLM For Official Use Only (FOUO) is no longer used. Sensitive: Cabinet DLM which referred to the Commonwealth Cabinet, is now a caveat and not a DLM. The other previous DLMs can be mapped directly to current NSW DLMs.

Figure 8: Mapping of old DLMs to new DLMs



6. Security classifications

A security classification (PROTECTED, SECRET and TOP SECRET) is only applied to information (or assets that hold information, such as laptops, USBs) if it requires protection because the impact of compromise of the information or asset would be high, extreme or catastrophic.

PROTECTED, SECRET and TOP SECRET are national security classifications and are subject to a memorandum of understanding between all states and the Australian Government.

Some NSW agencies will have their own PROTECTED, SECRET and TOP SECRET information. To assess which security classification to apply, a business impact levels (BIL) tool has been created as part of the Protective Security Policy Framework (PSPF) and should be considered when determining if information requires a security classification. The BIL tool can be found in Appendix 1.

Figure 9: Security classifications and BIL

PROTECTED	High business impact	***Damage*** to the national interest, organisations or individuals.
SECRET	Extreme business impact	***Serious damage*** to the national interest, organisations or individuals.
TOP SECRET	Catastrophic business impact	***Exceptionally grave damage*** to the national interest, organisations or individuals.

NSW agencies are required to handle this information according to the Australian Government requirements, including having the appropriate security clearances. NSW agency staff who handle PROTECTED, SECRET and TOP SECRET information must be security vetted.

When disclosing security classified information or resources to a person or organisation outside of government, agencies **must** have in place an agreement or arrangement, such as a contract or deed, governing how the information is used and protected.

To reduce the risk of unauthorised disclosure, agencies **must** ensure access to sensitive and security classified information or resources is only provided to people with a need-to-know.

Table 3: Security clearances required for ongoing access to PROTECTED, SECRET and TOP SECRET information

	Security classified information		
	PROTECTED	SECRET	TOP SECRET
Personnel security clearance for ongoing access	Baseline security clearance or above.	Negative Vetting 1 security clearance or above.	Negative Vetting 2 security clearance or above.

Agencies **must** ensure that people requiring access to caveated information meet all clearance and suitability requirements imposed by the originator and caveat owner.

6.1 Labelling of security classified information

The originator **must** clearly label security classified information, including emails (and associated metadata), unless impractical for operational reasons. Text-based labels are the preferred method using capitals, bold text, large font and a distinctive colour (red preferred), for example **OFFICIAL.**

The labels should be placed at the centre top and bottom of each page and if there is more than one label, for example a protective marking and a caveat, these need to be separated by a double forward slash (//). E.g., **PROTECTED//CABINET.**

The order for labelling is as follows:

1. classification (or the dissemination limiting marker)
2. foreign government information markings (if any)
3. caveats or other special handling instructions (if any) then
4. (optional) information management markers (IMM) (if any).

Paragraph grading indicators are useful where there is a need to identify the security classification of each individual paragraph or section, in addition to the document's overall protective marking or classification. Use of paragraph grading indicators is optional.

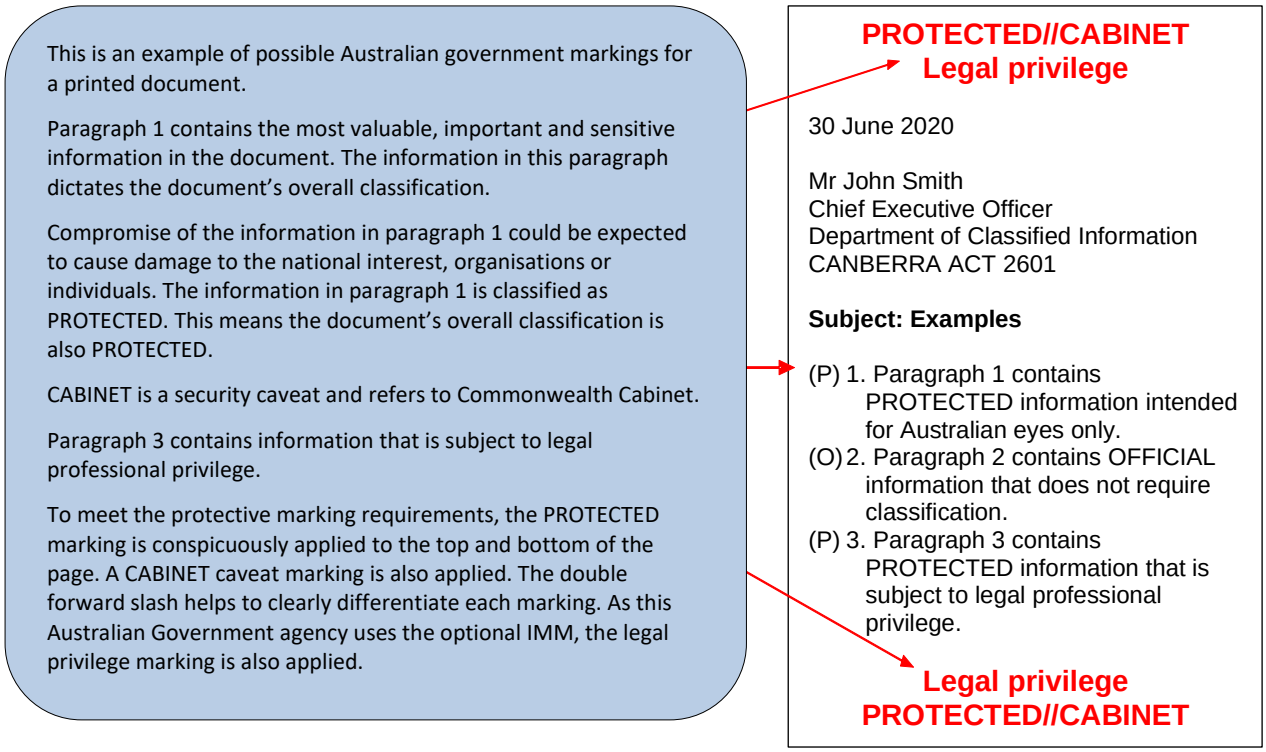
If used, paragraph grading indicators should:

- appear in the same colour as the text within the document either in:
  - brackets at the start or end of each paragraph, or
  - the margin adjacent to the first letter of the paragraph.
- be written in full or abbreviated by the first letter/s of the markings, as follows:
  - (UO) for UNOFFICIAL
  - (O) for OFFICIAL

- (O:S) for OFFICIAL: Sensitive
- (P) for PROTECTED
- (S) for SECRET
- (TS) for TOP SECRET.

The paragraph or section with the most valuable, important or sensitive information (highest classification) dictates the document's overall protective marking or classification.

Figure 10: Australian Government example of labelling physical (printed) information



If text-based protective markings cannot be used, use colour-based protective markings, or if text or colour-based protective markings cannot be used (e.g. verbal information), apply the agencies marking scheme for such scenarios. Agencies **must** document a marking scheme for this purpose and train personnel appropriately.

Colour-based markings use the RGB model, which refers to Red (R), Green (G) and Blue (B) colours that can be combined in various proportions to obtain any colour in the visible spectrum. Table 4 specifies the recommended RGB colour-based marking that applies to each security classification. There are no specific RGB colours for information labelled with a NSW DLM and OFFICIAL information, although a Yellow colour is recommended for DLMs.

Table 4: RGB cell colour for colour-based markings

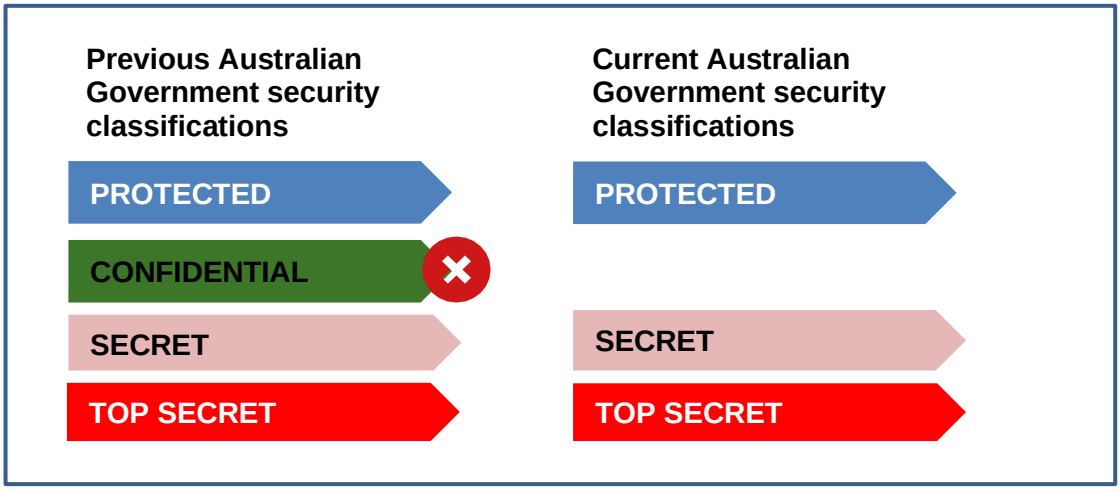
Security classification	Colour-based marking	RGB cell colour
PROTECTED	Blue	R 79, G 129, B 189
SECRET	Pink/Salmon	R 229, G 184, B 183
TOP SECRET	Red	R 255, G 0, B 0

6.2 Mapping from old security classifications to new security classifications

From October 2020, do not mark new information as CONFIDENTIAL. For new information that would previously have been marked CONFIDENTIAL, use the BIL tool, to determine the level of harm if information was compromised, and apply corresponding security classification marking under the current PSPF.

To handle existing information labelled as CONFIDENTIAL, please refer to the PSPF Annex F Table 3 Minimum protection and handling for CONFIDENTIAL information. The need-to-know principle applies to all CONFIDENTIAL information. Ongoing access to CONFIDENTIAL information requires a Negative Vetting 1 security clearance or above. Any temporary access must be supervised.

Figure 11: Previous and current Australian Government security classifications



6.2.1 I have information already labelled as CONFIDENTIAL do I need to re-label this information?

If this information is in use and the information was originally labelled by the agency, then it needs to be re-labelled. Refer to the BIL tool to determine if the impact of compromise is high, extreme or catastrophic. If the information is in use but came from another agency, then the originator of the information will need to change the label.

6.2.2 How do I manage information labelled as CONFIDENTIAL?

Access to CONFIDENTIAL information is need-to-know and needs a Negative Vetting 1 security clearance or above. The management of this information needs to be done in accordance with the PSPF CONFIDENTIAL minimum protection and handling guidelines.

6.2.3 I have information I would usually label as CONFIDENTIAL, what label do I need to apply now?

Use the BIL tool to determine which security classification to use.

6.2.4 The person who originally labelled the information CONFIDENTIAL no longer works here. Who should change the label?

The information custodian in your agency should reassess the information using the BIL tool to determine the new security classification.

6.3 Handling of security classified information

Agencies handling security classified information must refer to the PSPF handling guidelines which have been appended to this report (Appendices 2, 3 and 4).

NSW agencies must retain records and information in accordance with the *State Records Act 1998* (NSW) and any other legal and accountability requirements. Agencies should refer to applicable Functional Retention and Disposal Authorities and General Retention and Disposal Authorities. See NSW State Archives and Records' website for further information on retention and disposal authorities, and guidance on information/record retention, disposal, physical storage of paper records and archiving.

Guidelines on cyber security are available from the Australian Signals Directorate, Australian Cyber Security Centre.

6.3.1 How do I know if my system is able to store sensitive or security classified information?

Agency ICT systems can be certified for PROTECTED and OFFICIAL systems, SECRET or TOP SECRET systems. The determining authority for security assessment (assessor) is the Agency's Security Advisor (ASA), and the certification authority is the Chief Security Officer (or delegated security advisor).

Agency ICT systems should be audited, and a security assessment completed to identify any potential deficiencies and considers the effectiveness of security protections. A certification certifies that the security measures have been implemented and are operating effectively. Further information can be found in the Australian Government Information Security Manual.

7. Caveats and accountable material

The caveat is a warning that the information has special protections in addition to those indicated by the security classification. Caveats are not classifications and must appear with an appropriate security classification marked as text.

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.

The Australian Government Security Caveats Guidelines establishes four categories of caveats:

1. codewords (sensitive compartment information)
2. foreign government markings
3. special handling instructions
4. releasability caveats.

The Australian Government mandates that caveated information and accountable material be clearly marked and handled in accordance with the originator and the caveat holder's special handling requirements as established in the Australian Government Security Caveats Guidelines. These special caveat requirements apply in addition to the classification handling requirements.

Australian Government accountable material is information that requires the strictest control over its access and movement. Accountable material includes:

- TOP SECRET security classified information
- some types of caveated information, being:
    - all codeword information
    - select special handling instruction caveats, particularly CABINET (Cth) information at any security classification
    - any classified information designated as accountable material by the originator.

What constitutes accountable material may vary from Australian Government entity to entity and could include budget papers, tender documents and sensitive ministerial briefing documents.

Entities **must** ensure that accountable material:

- has page and reference numbering
- is handled in accordance with any special handling requirements imposed by the originator and caveat owner
- has an auditable record of all incoming and outgoing material, transfer, copy or movements.

Additional information about handling caveats is available in the Sensitive Material Security Management Protocol. Both the Australian Government Security Caveats Guidelines and the Sensitive Material Security Management Protocol documents are available on a need-to-know basis on the GovTEAMS site. If NSW agencies are receiving or using caveated or accountable material these guidelines and protocols must be followed.

8. Information management markers

(Optional and not applied to NSW information)

The Australian Government PSPF has introduced the use of information management markers (IMM). IMM are an **optional** way for Australian government agencies to identify information that is subject to non-security related restrictions on access and use. IMM are not protective markers. They are a subset of the controlled list of terms for the 'Rights Type' property in the National Archives of Australia's Australian Government Recordkeeping Metadata Standard (AGRkMS).

The Australian Government has three IMM which can be used with OFFICIAL: Sensitive, PROTECTED, SECRET or TOP SECRET classifications.

1. **Legal privilege**: This is used if the information is subject to legal professional privilege.
2. **Personal privacy:** This is used if the information is personal information as defined in the *Privacy Act 1988*. This refers to Commonwealth legislation and includes information which is both private and health information.
3. **Legislative secrecy**: This is used if the information is subject to one or more legislative secrecy provisions.

8.1 Application of IMM in NSW

NSW agencies are not to apply IMMs to NSW information.

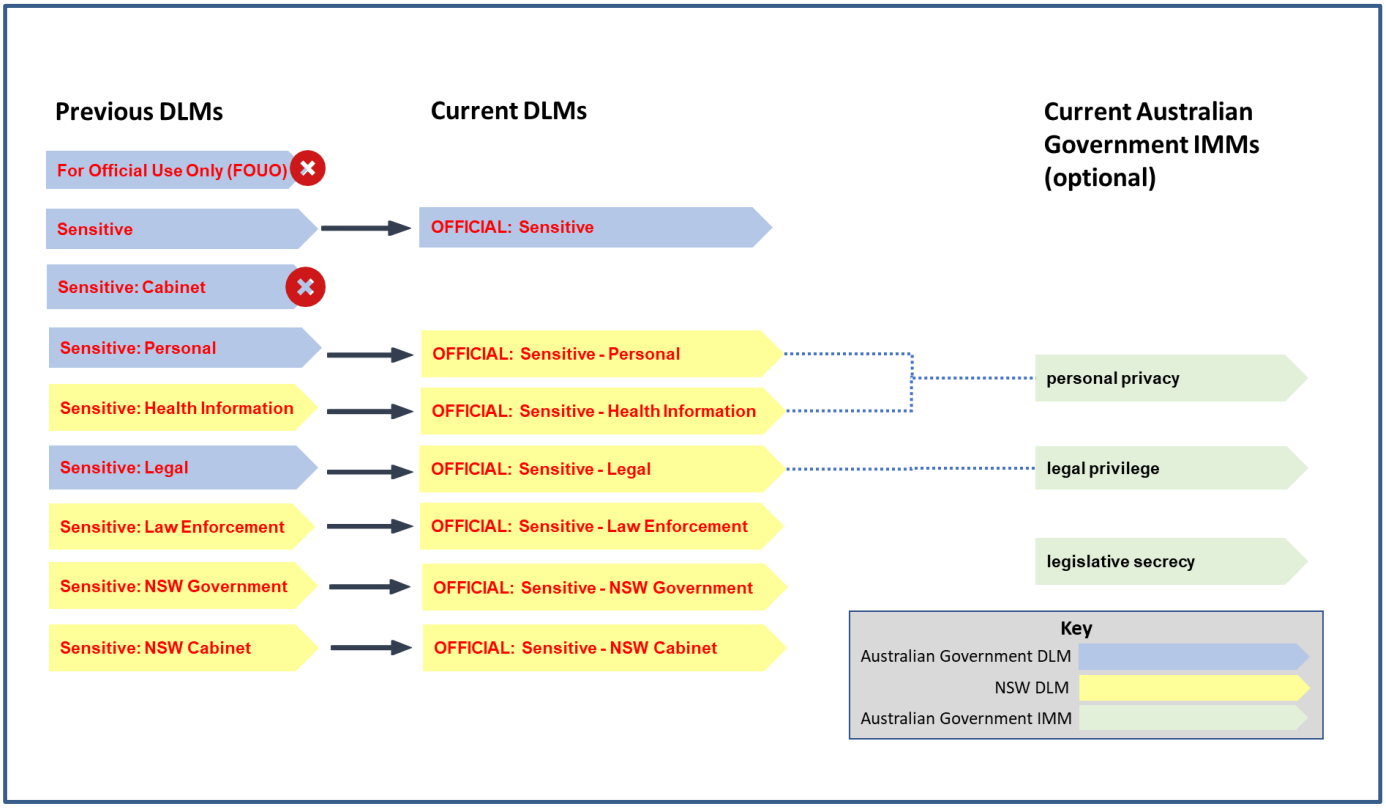
*Information management markers (IMM) are **not** applied to NSW information.*

Figure 12: shows the relationship between previous Australian Government Dissemination Limiting Markers (DLMs), NSW DLMs and the new Australian Government IMMs.

Sensitive: Legal was an Australian Government DLM and this has now changed to an IMM. This IMM could align to the NSW DLM 'OFFICIAL: Sensitive Legal' as both label information which is subject to legal professional privilege.

Previously the Australian Government had a DLM 'Sensitive – personal' and NSW had an additional DLM 'Sensitive – Health Information'. NSW is continuing to apply both DLMs and these could align to the new IMM personal privacy. The reason NSW has opted for two DLMs to protect personal and health information is because there are two separate pieces of legislation which describe this information, whereas the Commonwealth has one.

Figure 12: Dissemination Limiting Markers (DLM) and Information Management Markers (IMM)



The legislative secrecy IMM is new and does not directly align to NSW DLMs. NSW has many pieces of legislation which contain preservation of secrecy, secrecy clauses and disclosure of information clauses and there is potential for information associated with these clauses to be labelled with an IMM.

Preservation of secrecy, secrecy clauses and disclosure of information clauses are similar in that they limit the disclosure of information to another person, and often state who has the right to provide the permission to disclose that information. For example some Acts state that permission for disclosure could be granted by the responsible Minister. Secrecy and disclosure clauses are aimed to protect the individual, law enforcement activities, an investigation or proprietary rights.

Protective marking labels with IMMs from the Australian Government other states could look like this:

- OFFICIAL: Sensitive – legal privilege
- OFFICIAL: Sensitive – legislative secrecy
- OFFICIAL: Sensitive – personal privacy.

8.2 What do the IMM mean?

Information management markers are essentially an alert to let the user of the information know that there are additional restrictions on the use and sharing of the information.

8.3 Do I need to apply IMM in NSW?

No, information management markers are not applied to NSW information.

8.4 How do I manage Australian Government information marked with an IMM?

The information needs to be stored with the information management marker and then managed according to the level of sensitivity or security classification.

8.5 Do I need to re-label Australian Government information if it has an IMM?

No, you do not need to re-label the information.

8.6 I am sending information to the Australian Government; do I add an IMM?

No, apply appropriate NSW DLM or security classification.

9. Definition of terms

Accountable material: In the 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.

Investigative agency:
The *Privacy and Personal Information Protection Act 1998* No 133 define an investigative agency as:

a. meaning any of the following:

- Ombudsman's Office
- Independent Commission Against Corruption
- Inspector of the Independent Commission Against Corruption
- Law Enforcement Conduct Commission
- Inspector of the Law Enforcement Conduct Commission and any staff of the Inspector
- Health Care Complaints Commission
- Office of the Legal Services Commissioner
- Ageing and Disability Commissioner
- Children's Guardian
- a person or body prescribed by the regulations for the purposes of this definition.

b. any other public sector agency with investigative functions if:

- those functions are exercisable under the authority of an Act or statutory rule (or where that authority is necessarily implied or reasonably contemplated under an Act or statutory rule)
- the exercise of those functions may result in the agency taking or instituting disciplinary, criminal or other formal action or proceedings against a person or body under investigation.

c. a public sector agency conducting an investigation on behalf of an agency referred to in paragraph (a) or (b).

Law enforcement agency means:

a. the NSW Police Force or the police force of another state or territory or of an overseas jurisdiction
b. the Australian Federal Police

c. the New South Wales Crime Commission
d. the Australian Criminal Intelligence Commission
e. any other authority or person responsible for the investigation or prosecution of offences against the laws of the state or of the Commonwealth, another state or territory or an overseas jurisdiction.

Need-to-know: 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.

Originator: The person or agency responsible for generating, preparing or actioning information is called the Originator.

Safe hand: Carriage of protectively marked information by safe hand means 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 (see the Protective Security Policy Framework for guidance).

Security zones: The 16 Entity facilities policy describes a consistent and structured approach to be applied to building construction, security zoning and physical security control measures of entity facilities. This ensures the protection of Australian Government people, information and physical assets secured by those facilities.

When designing or modifying facilities, entities **must**:

- secure and control access to facilities to meet the highest risk level to entity resources
- define restricted access areas as detailed below.

Zone name	Zone definition
Zone 1	Public access.
Zone 2	Restricted public access. Unrestricted access for authorised personnel. May use single factor authentication for access control.
Zone 3	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel. Single factor authentication for access control.
Zone 4	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Single factor authentication for access control.
Zone 5	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Dual factor authentication for access control.

10. Acronyms

BIL: Business impact levels tool – this tool can be used to assess the potential damage to the national interest, government, organisations or individuals, of unauthorised release of information.

DLM: Dissemination limiting marker.

eCabinet: This is the name of the information management system managed by the NSW Department of Premier and Cabinet.

IMM: Information management markers.

MoU: Memorandum of understanding.

PSM: Protective Security Manual. This document was superseded by the PSPF.

PSPF: Protective Security Policy Framework. This framework was developed by the Australian Government Attorney-General's Department and consists of a number of policy documents which describe the governance, information, personnel and physical requirements to protect people, information and assets, at home and overseas.

Appendix 1. NSW Business Impact Levels tool

Table 1: Business Impact Levels tool		Sensitive information	Security classified information		
	OFFICIAL	DLM with prefix: OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Sub-impact category ↓	**Most official information created or processed by the public sector. This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in no or insignificant damage to individuals, organisations or government.**	**OFFICIAL information that due to its sensitive nature requires limited dissemination. Information with a prefix of OFFICIAL: Sensitive is not a security classification. It is a dissemination limiting marker (DLM), indicating compromise of the information would result in limited damage to an individual, organisation or government.**	**Valuable, important and sensitive information. Compromise of PROTECTED information would be expected to cause damage to the national interest, organisations or individuals.**	**Very valuable, important and sensitive information. Compromise of SECRET information would be expected to cause serious damage to the national interest, organisations or individuals.**	**The most valuable, important and sensitive information. Compromise of TOP SECRET information would be expected to cause exceptionally grave damage to the national interest, organisations or individuals.**
Potential impact on individuals from compromise of the information					
Dignity or safety of an individual (or those associated with the individual)	Information from routine business operations and services. Can include personal information but excludes sensitive information as defined under the *Privacy Act* (Cth). Note: NSW privacy legislation (HRIPA and PPIPA) do not have a definition for sensitive information.	Limited damage to an individual is: a. potential harm, for example injuries that are not serious or life threatening or b. discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is not life threatening.	Damage to an individual is discrimination, mistreatment, humiliation or undermining of an individual's dignity or safety that leads to potentially **significant harm or potentially life-threatening injury**.	Serious damage is discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to **directly threaten or lead to the loss of life of an individual or small group**.	Exceptionally grave damage is: a. widespread loss of life b. discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly lead to the death of a large number of people.
Potential impact on organisations from compromise of the information					
Entity operations, capability and service delivery	Information from routine business operations and services.	Limited damage to entity operations is: a. a degradation in organisational capability to an extent and duration that, while the **entity can perform its primary functions**, the effectiveness of the functions is noticeably reduced b. minor loss of confidence in government.	Damage to entity operations is: a. a degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform one or more of its primary functions** b. major loss of confidence in government.	Serious damage to entity operations is: a. a severe degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform any of its functions** b. directly threatening the internal stability of Australia.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Entity assets and finances, e.g. operating budget	Information compromise would result in insignificant impact to the entity assets or annual operating budget.	Limited damage to entity assets or annual operating budget is equivalent to $**10 million to $100 million**.	Damage is: a. substantial financial loss to an entity b. **$100 million to $10 billion** damage to entity assets.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Legal compliance, e.g. information compromise would cause non-compliance with legislation, commercial confidentiality or legal professional privilege	Information compromise would not result in legal and compliance issues.	Limited damage is: a. issues of legal professional privilege for communications between legal practitioners and their clients b. contract or agreement non-compliance c. failure of statutory duty d. breaches of information disclosure limitations under legislation resulting in less than two years' imprisonment.	Damage is: a. failure of statutory duty or breaches of information disclosure limitations under legislation resulting in two or more years' imprisonment.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to the compromise of information are assessed as to the level of impact to the national interest.
Compiled data[i]	A compilation of routine business information.	A significant compiled holding of information that, if compromised, would cause limited damage to the national interest, organisations or individuals.	A significant compiled holding of sensitive information that, if compromised, would cause damage to the national interest, organisations or individuals.	A significant compiled holding of sensitive or classified information that, if compromised, would cause serious damage to the national interest, organisations or individuals.	A significant compiled holding of sensitive or classified information that, if compromised, would cause exceptionally grave damage to the national interest, organisations or individuals.
Potential impact on government or the national interest from compromise of the information					
Policies and legislation	Information compromise from routine business operations and services. For example, this may include information	Limited damage to government is impeding the development or operation of policies.	Damage to the national interest is: a. impeding the development or operation of major policies	Serious damage to the national interest is: a. a severe degradation in development or operation of multiple major policies to an	Exceptionally grave damage to the national interest is the collapse of internal political stability of Australia or friendly countries.

Table 1: Business Impact Levels tool		Sensitive information	Security classified information		
	OFFICIAL	DLM with prefix: OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Sub-impact category ↓	**Most official information created or processed by the public sector. This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in no or insignificant damage to individuals, organisations or government.**	**OFFICIAL information that due to its sensitive nature requires limited dissemination. Information with a prefix of OFFICIAL: Sensitive is not a security classification. It is a dissemination limiting marker (DLM), indicating compromise of the information would result in limited damage to an individual, organisation or government.**	**Valuable, important and sensitive information. Compromise of PROTECTED information would be expected to cause damage to the national interest, organisations or individuals.**	**Very valuable, important and sensitive information. Compromise of SECRET information would be expected to cause serious damage to the national interest, organisations or individuals.**	**The most valuable, important and sensitive information. Compromise of TOP SECRET information would be expected to cause exceptionally grave damage to the national interest, organisations or individuals.**
	in a draft format (not otherwise captured by higher business impact level).		b. revealing deliberations or decisions of cabinet, or matters submitted, or proposed to be submitted, to cabinet (Cth)[iv] (not otherwise captured by (higher level business impacts).	extent and duration that the policies can no longer be delivered.	
Australian economy	Information from routine business operations and services.	Limited damage to government is: a. undermining the financial viability of one or more individuals, minor Australian-based or owned organisations or companies b. disadvantaging a major Australian organisation or company.	Damage to the national interest is: a. undermining the financial viability of a major Australian-based or owned organisation or company b. disadvantaging some major Australian organisations or companies c. short-term material impact on national finances or economy.	Serious damage to the national interest is: a. undermining the financial viability of an Australian industry sector (multiple major organisations in the same sector) b. long-term damage to the Australian economy to an estimated total in excess of $20 billion.	Exceptionally grave damage to the national interest is the collapse of the Australian economy.
National infrastructure	Information from routine business operations and services.	Limited damage to government is damaging or disrupting state or territory infrastructure.	Damage to the national interest is damaging or disrupting significant state or territory infrastructure.	Serious damage to the national interest is shutting down or substantially disrupting significant national infrastructure.	Exceptionally grave damage to the national interest is the collapse of all significant national infrastructure.
International relations	Information from routine business operations and diplomatic activities.	Limited damage to government is minor and incidental damage or disruption to diplomatic relations.	Damage to the national interest is: a. short-term damage or disruption to diplomatic relations b. disadvantaging Australia in international negotiations or strategy.	Serious damage to the national interest is: a. severely disadvantaging Australia in major international negotiations or strategy b. directly threatening internal stability of friendly countries, leading to widespread instability c. raising international tension or severely disrupting diplomatic relations resulting in formal protest or sanction.	Exceptionally grave damage to the national interest is directly provoking international conflict or causing exceptionally grave damage to relations with friendly countries.
Crime prevention, defence or intelligence operations	Information from routine business operations and services.	Limited damage to government is: a. impeding the detection, investigation, prosecution of, or facilitating the commission of low-level crime b. affecting the non-operational effectiveness of Australian or allied forces without causing risk to life. c. Impeding the safe and secure management of offenders and detention facilities without causing risk of life.	Damage to the national interest is: a. impeding the detection, investigation, prosecution of, or facilitating the commission of an offence with two or more years imprisonment[vi]- *when it causes damage to the national interest.* b. affecting the non-operational effectiveness of Australian or allied forces that could result in risk to life. c. Impeding the safe and secure management of offenders and detention facilities that could result in risk of life.	Serious damage to the national interest is major long-term impairment to the ability to investigate or prosecute serious organised crime[v] affecting the operational effectiveness, security or intelligence capability of Australian or allied forces.	Exceptionally grave damage to the national interest is significantly affecting the operational effectiveness, security or intelligence operations of Australian or allied forces.

i Note the PSPF refers to this sub-category as aggregated data. The definition used by the PSPF for aggregated data is: A compilation of information may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications.

[iv] This includes official records of cabinet, cabinet business lists, minutes, submissions, memoranda or matters without submission, and any other information that has been submitted or proposed to be submitted to cabinet.

[v] Serious organised crime as defined in the Convention Against Transnational Organised Crime.

[VI] In NSW a. is interpreted as Major Crime of significant public interest and/or when it causes damage to the national interest.

Appendix 2. Minimum protections and handling of TOP SECRET information[1]

Business Impact Levels (BIL) 5	TOP SECRET—exceptionally grave damage to the national interest, organisations or individuals
Protective marking	Apply text-based protective marking **TOP SECRET** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For TOP SECRET a red colour is recommended. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. If marking paragraphs, it is recommended that TOP SECRET is written in full or abbreviated to (TS) and placed either in brackets at the start or end of the paragraph or in the margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle applies to all TOP SECRET information. Ongoing access to TOP SECRET information requires a Negative Vetting 2 security clearance or above. Any temporary access must only be provided to personnel with at least a Negative Vetting 1 security clearance and must be supervised.
Use	TOP SECRET information can only be used in Zones 3-5. **Outside entity facilities (including at home)** **Do not** use outside entity facilities (including at home).
Storage	**Do not** leave TOP SECRET information, or a mobile device that processes, stores or communicates TOP SECRET information, unattended. Store securely when unattended. When storing TOP SECRET information, or a mobile device that processes, stores or communicates TOP SECRET information: a. inside entity facilities: i. Zone 5, store in Class B container ii. Zones 3-4, store in exceptional circumstances only for a maximum of 5 days, Zone 4 (in Class B container) or Zone 3 (in a Class A container). b. outside entity facilities: **do not** store TOP SECRET information, or a mobile device that processes, stores or communicates TOP SECRET information, outside entity facilities (including at home).
Carry	When carrying physical TOP SECRET information **always retain it in personal custody** a. inside entity facilities: i. Zones 3-5, in an opaque envelope or folder that indicates classification ii. Zones 1-2, **not recommended**, if required, in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: **not recommended**, if required:

[1] Refer to the online version of the PSPF for to most up to date minimum protections and handling guides. https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx

	i. obtain written manager approval ii. place in tamper-evident packaging within a security briefcase, pouch or satchel. Mobile devices that that process, store or communicate TOP SECRET information require explicit approval by the Australian Signals Directorate (ASD). When carrying an approved TOP SECRET mobile device **always retain it in personal custody** a. inside entity facilities: i. Zones 3-5, carry in secured state; if in an unsecured state apply entity procedures ii. Zones 1-2, carry in a secured state; if in an unsecured state, place inside a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities – **not recommended**, if required: i. obtain written manager approval ii. carry in a secured state; if in an unsecured state, place in tamper-evident packaging within a security briefcase, pouch or satchel.
Transfer	When transferring physical TOP SECRET information a. inside entity facilities i. Zones 3-5, transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if in close proximity and the office environment presents low risk of unauthorised viewing ii. Zones 1-2, transfer by hand or entity safe hand and apply requirements for carrying with written manager approval. b. to another officer in a different facility i. obtain written manager approval ii. apply requirements for carrying outside entity facilities (including using tamper evident packaging) iii. transfer by hand, entity safe hand, safe hand courier rated BIL 5, or DFAT courier. Any transfer requires a receipt.
Transmit	When transmitting electronically, communicate information over TOP SECRET secure networks. Use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information for any communication that is not over a TOP SECRET network.
Official travel	TOP SECRET information and mobile devices that process, store or communicate TOP SECRET information **must not** be stored or used outside appropriate entity facilities. **Travel in Australia** Travelling domestically with physical TOP SECRET information is **not recommended**, if required: a. obtain written manager approval b. apply requirements for carrying outside entity facilities and any additional entity procedures c. for airline travel, retain as carry-on baggage and **do not travel** if the airline requires it to be checked at the gate. **Do not** leave TOP SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility. Travelling domestically with a mobile device that processes, stores or communicates TOP SECRET information is **not recommended**, consider alternative options to access information at destination. If required: a. obtain written manager approval b. apply requirements for carrying outside entity facilities and any additional entity procedures

	c. for airline travel, retain as carry-on baggage; if airline requires carry-on baggage to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim as soon as possible. **Do not** leave device unattended. **Do not** store device while travelling (eg in a hotel room). If storage required, store in an Australian entity facility. **Travel outside Australia** **Do not** travel overseas with TOP SECRET information or a mobile device that processes, stores or communicates TOP SECRET information, seek DFAT advice on options to access information or mobile devices at overseas destination. If access to TOP SECRET information or mobile device provided at overseas destination: a. apply requirements for carrying outside entity facilities and any additional entity procedures b. retain in personal custody or store in an Australian entity facility. **Do not** leave TOP SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility.
Disposal	Dispose of TOP SECRET information using a Class A shredder – supervise and document destruction

Appendix 3. Minimum protections and handling of SECRET information

Business Impact Levels (BIL) 4	SECRET—serious damage to national interest, organisations or individuals
Protective marking	Apply text-based protective marking **SECRET** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For SECRET a salmon pink colour is recommended. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. If marking paragraphs, it is recommended that SECRET is written in full or abbreviated to (S) and placed either in brackets at the start or end of the paragraph or in the margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle applies to all SECRET information. Ongoing access to SECRET information requires a Negative Vetting 1 security clearance or above. Any temporary access must be supervised.
Use	SECRET information and mobile devices that process, store or communicate SECRET information can be used in security Zones 2-5. **Outside entity facilities (including at home)** **Do not** use SECRET information and mobile device that processes, stores or communicates SECRET information for regular ongoing home-based work a. Occasional home-based work is **not recommended**, if required: i. obtain manager approval ii. apply entity procedures on need for a security assessment iii. exercise judgement to assess environment risk **Do not** use SECRET information and mobile device that processes, stores or communicates SECRET information anywhere else outside entity facilities (for example private sector offices, café).
Storage	**Do not** leave SECRET information or a mobile device that processes, stores or communicates SECRET information unattended. Store securely when unattended. When storing physical SECRET information: a. inside entity facilities (Zones 3-5 only): i. Zones 4-5, store in Class C container ii. Zone 3, store in Class B container. b. outside entity facilities: **not recommended**, if required for occasional home-based work (see use above): i. apply requirements for carrying outside entity facilities ii. retain in personal custody (strongly preferred), or for brief absences from home, store in a Class B or higher container that has been approved as a proper place of custody by the Accountable Authority or their delegate iii. return to entity facility as soon as practicable. When storing a mobile device that processes, stores or communicates SECRET information:

	a. inside entity facilities (Zones 2-5 only): i. Zones 4-5: if in a secured or unsecured state, store in Class C container ii. Zone 3: if in a secured state, Class C container, if unsecured state, store in Class B container iii. Zone 2: if in a secured state, Class B container, if unsecured state, store in a higher zone. b. outside entity facilities **not recommended**, if required for occasional home-based work (see use above): i. apply requirements for carrying outside entity facilities ii. retain in personal custody (strongly preferred), or for brief absences from home, exercise judgement to store in a Class C or higher container that has been approved as a proper place of custody by the Accountable Authority or their delegate.
Carry	When carrying physical SECRET information **always retain it in personal custody** a. inside entity facilities: i. Zones 2-5, carry in an opaque envelope or folder that indicates classification ii. Zone 1, carry in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: i. place in a security briefcase, pouch or satchel ii. **recommend** tamper-evident packaging if aggregate information increases risk When carrying a mobile device that processes, stores or communicates SECRET information **always retain it in personal custody** a. inside entity facilities: i. Zone 5, if in a secured or unsecured state, apply entity procedures ii. Zones 2-4, carry in secured state; if in an unsecured state, apply entity in procedures iii. Zone 1, carry in a secured state; if in an unsecured state, place inside a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: i. carry in a secured state; if in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper evident seals.
Transfer	When transferring SECRET information: a. inside entity facilities (Zones 1-5): transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if office environment presents very low risk of unauthorised viewing b. to another officer in a different facility: i. apply requirements for carrying outside entity facilities ii. transfer by hand, entity safe hand, safe hand courier rated BIL 4, or DFAT courier (if transfer by courier, use tamper evident packaging). Any transfer requires a receipt.
Transmit	When transmitting electronically, communicate over SECRET secure networks (or networks of higher classification). Use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information for any communication that is not over a SECRET network (or network of higher classification).
Official travel	**Travel in Australia** Travelling domestically with SECRET information or with a mobile device that processes, stores or communicates SECRET information is **not recommended**. If required: a. apply requirements for carrying outside entity facilities and any additional entity procedures b. for airline travel, retain as carry-on baggage; if airline requires carry-on baggage to be checked at the gate,

	i. place in tamper-evident packaging within a security briefcase, pouch or satchel and try to observe entering and exiting the cargo hold and reclaim as soon as possible ii. if tamper-evident packaging not available, **do not travel**. **Do not** leave SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility. **Travel outside Australia** Travelling overseas with SECRET information, or with a mobile device that processes, stores or communicates SECRET information, is **not recommended**—seek DFAT advice on options to access information at destination. If travel with SECRET information or mobile device is required: a. apply requirements for carrying outside entity facilities and any additional entity procedures (entities can consult DFAT for assistance in establishing procedures), consider country-specific travel advice b. for airline travel, retain as carry-on baggage and **do not travel** if the airline requires it to be checked at the gate. If access to SECRET information or mobile device provided at destination: a. apply requirements for carrying outside entity facilities and any additional entity procedures b. retain in personal custody or store in an Australian entity facility. **Do not** leave SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility.
Disposal	Dispose of SECRET information using a Class A shredder.

Appendix 4. Minimum protections and handling of PROTECTED information

Business Impact Levels (BIL) 3	PROTECTED—damage to the national interest, organisations or individuals
Protective marking	Apply text-based protective marking **PROTECTED** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For PROTECTED a blue colour is recommended. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. If marking paragraphs, it is recommended that PROTECTED is written in full or abbreviated to (P) and placed either in brackets at the start or end of the paragraph or in the margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle applies to all PROTECTED information. Ongoing access to PROTECTED information requires a Baseline security clearance or above. Any temporary access must be supervised.
Use	PROTECTED information and mobile devices that process, store or communicate PROTECTED information can be used in Zones 1-5. **Outside entity facilities (including at home)** PROTECTED information and mobile devices that process, store or communicate PROTECTED information: a. For regular ongoing home-based work, apply entity procedures, which must include conducting a security risk assessment of the proposed work environment b. For occasional home-based work, apply entity procedures on need for a security assessment and exercise judgement to assess environmental risk c. For anywhere else outside entity facilities (for example private sector offices, café): i. use of physical PROTECTED information is **not recommended**, if required, apply entity procedures and exercise judgement to assess environmental risk ii. use of mobile device that process, store or communicate PROTECTED information: apply entity procedures and exercise judgement to assess environmental risk
Storage	**Do not** leave physical PROTECTED information unattended, store securely when unattended. Mobile devices that process, store or communicate PROTECTED information can be left unattended if in a secured state, subject to entity clear desk policy. When storing physical PROTECTED information: a. inside entity facilities (Zones 2-5 only): i. Zones 4-5, store in lockable container ii. Zones 2-3, store in Class C container b. outside entity facilities: i. for regular ongoing home-based work, install and store in a Class C or higher container ii. occasional home-based work, apply requirements for carrying outside entity facilities, and retain in personal custody (strongly preferred), or for brief absences

	from home, apply entity procedures and exercise judgement to assess environmental risk. When storing a mobile device that processes, stores or communicates PROTECTED information a. inside entity facilities (Zones 1-5): i. Zones 4-5: if in a secured state, **recommend** storing in lockable container; if in an unsecured state, store in lockable container ii. Zone 2-3: if in a secured state, **recommend** storing in lockable container; if in an unsecured state, store in Class C container iii. Zone 1: if in a secured state, store in Class C container, if unsecured state, store in a higher zone. b. outside entity facilities: i. for regular ongoing and occasional home-based work, apply entity procedures and exercise judgement to assess environment risk ii. if in a secured state, **recommend** store in in lockable container; if in an unsecured state, store in a Class C or higher container.
Carry	When carrying physical PROTECTED information **always retain it in personal custody** a. inside entity facilities: i. Zones 1-5, in an opaque envelope or folder that indicates classification b. outside entity facilities (including external meetings) and between entity facilities: i. place in a security briefcase, pouch or satchel ii. **recommend** using tamper-evident packaging if aggregate information increases risk. When carrying a mobile device that processes, stores or communicates PROTECTED information a. inside entity facilities: i. Zone 2-5, if in a secured or unsecured state, apply entity procedures ii. Zone 1, carry in secured state; if in an unsecured state, apply entity in procedures b. outside entity facilities (including external meetings) and between entity facilities: i. carry in a secured state; if in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper-evident packaging.
Transfer	When transferring PROTECTED information a. inside entity facilities (Zones 1-5): transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if office environment presents low risk of unauthorised viewing b. to another officer in a different facility i. apply requirements for carrying outside entity facilities ii. transfer by hand, entity safe hand, safe hand courier rated BIL 4, or DFAT courier (if transfer by courier, use tamper evident packaging). Any transfer requires a receipt.
Transmit	When transmitting electronically communicate information over PROTECTED networks (or networks of higher classification). Encrypt PROTECTED information for any communication that is not over a PROTECTED network (or network of higher classification).
Official travel	**Travel in Australia** PROTECTED information can be taken to external meetings and on domestic travel. When travelling with PROTECTED information or a mobile device that processes, stores or communicates PROTECTED information: a. apply requirements for carrying outside entity facilities and any additional entity procedures

	b. for airline travel, retain as carry-on baggage; if airline requires to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim as soon as possible Leaving PROTECTED information, or a mobile device that processes, stores or communicates PROTECTED information, unattended while travelling is **not recommended**. For brief absences from a hotel room, apply entity procedures and exercise judgement to assess environmental risk. **Travel outside Australia** Travelling overseas with physical PROTECTED information is **not recommended**—seek DFAT advice on options to access information at destination. If travel with physical PROTECTED information is required or when travelling a mobile device that processes, stores or communicates PROTECTED information: a. apply requirements for carrying outside entity facilities and any additional entity procedures (entities can consult DFAT for assistance in establishing procedures) and consider country-specific travel advice b. for airline travel, retain as carry-on baggage and **do not travel** if the airline requires it to be checked at the gate. **Do not** leave PROTECTED information or device unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility.
Disposal	Dispose of PROTECTED information using a Class B shredder.

Document Version Control

Version	Date	Prepared by	Comments
1.0	15.07.2020	Elizabeth de Vries	Final draft incorporating working group comments.
2.0	06.08.2020	Elizabeth de Vries	Final incorporating final working group comments.
2.1	02.10.2020	Elizabeth de Vries	Updating links to NSW Government Legislation website

Customer, Delivery & Transformation, Department of Customer Service

Address: McKell Building 2-24 Rawson Place, Sydney NSW 2000

Phone: 13 77 88 | TTY: 1300 301 181

www.customerservice.nsw.gov.au