Please note, this document is under review (2019).

Email: datansw@finance.nsw.gov.au for further information.

NSW Government Information Classification, Labelling and Handling Guidelines

July 2015

Department of Finance, Services and Innovation
Level 23, McKell Building
2-24 Rawson Place
SYDNEY NSW 2000

August 2015

Table of Contents

1. Document Control

Document Approval

Name & Position	Signature	Date

Document Version Control

Version	Status	Date	Prepared By	Comments
0.1	Consultation Draft	28 May 2013	DFS	Initial draft.
0.2	Consultation Draft	5 July 2013	DFS	Updated to reflect preferred options.
0.3	Draft	24 July 2013	DFS	Updated after input from the Information Security Steering Group and the Classification & Labelling Working Group.
0.4	Draft	30 August 2013	DFS	Further updated version taking in comments from DPC et al.
1.0	Final	September 2013	DFS	Final additional comments taken in.
1.1	Final	October 2013	DFS	Updated to reflect changes to the PSPF Business Impact Levels (BILs), and consequential minor amendments, affecting 3.6, 5.2, 5.3, 5.4, 5.5, 6.7 and Appendix D.
2.0	Draft	April 2015	OFS	Version 2 draft. Updated to incorporate the Classification Handling Guidelines and two new DLMs.
2.1	Draft	May 2015	OFS	Updated after input from the Information Security Steering Group
2.2	Final	July 2015	DFSI	Updated including DFSI branding

Review Date

These guidelines will be reviewed in July 2016.

They may be reviewed earlier in response to post-implementation feedback or as necessary.

2. Background

2.1 Purpose

The *NSW Government Digital Information Security Policy* (DISP) outlines the NSW Government's commitment to a system for classifying, labelling and handling sensitive information in a manner consistent with the Australian Government security classification system (the Australian Government System).

The *NSW Government Information Classification, Labelling and Handling Guidelines* (the Guidelines) help agencies identify the confidentiality requirements of their information assets and apply suitable protective markings.

The Guidelines align with the Australian Government *Protective Security Policy Framework* (PSPF), which provides controls for effectively managing the protective security risks to Government business. Specifically, the Guidelines are informed by the *Information security management guidelines – Australian Government security classification system*, which is a key component of the PSPF information security management policy.

The Guidelines are intended for use by agency information management professionals, including information security, records management, privacy and legal professionals. It is intended that the Guidelines will inform agency-specific information classification and handling policy and guidance for use by non-information management professionals.

2.2 Scope

In accordance with the scope and objectives of the DISP, this guidance applies to the classification, labelling and handling of sensitive information in any format, including records in physical and digital format. Agencies must refer to the relevant requirements in the PSPF for classifying and handling security classified information, i.e. **PROTECTED**, **CONFIDENTIAL**, **SECRET**, and **TOP SECRET** – particularly in relation to information affecting national security.

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 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.

Terms not explained within the text of the Guidelines are defined in the Glossary of Key Terms at **Appendix A**.

2.3 Background

Sharing information between State Government and Commonwealth Government agencies can have considerable benefits including, but not limited to, better service delivery, reduced duplication and subsequent costs, increased productivity and efficiency, improved inter-agency and cross-jurisdictional relationships, and better control of information.

Implementing consistent methods of classification and labelling allows sensitive information to be securely shared across jurisdictions, with confidence that the information will be handled and protected according to its sensitivity. This can support the delivery of emergency services, enable more effective law enforcement and contribute to national security operations. For this reason, the Guidelines align with the Australian Government System.

The Guidelines have been developed to:

- provide a consistent and structured approach to the classification and labelling of sensitive information to be used by all NSW agencies
- allow for integration between the existing sensitive information labels in NSW and the information security classification markings used by the Australian Government
- provide guidance for NSW agencies in transitioning to the system outlined in the Guidelines
- assist agencies in identifying security classified or sensitive information, and in applying appropriate protective markings to this information
- clarify where classification and labelling systems overlap
- encourage better practices in protective security procedures by all NSW agencies

The Guidelines are based on the *Information security management guidelines – Australian Government security classification system* and other components of the Australian Government PSPF. Where text from the Australian Government system is reproduced, specific attribution is not given in the Guidelines.

2.4 Superseded NSW guidance

The Guidelines supersede *C2002-69 NSW Guide to Labelling Sensitive Information 2011 Version 1.2* (30/6/2011).

Information labelled or classified before 1 July 2015 does not need to be re-labelled or reclassified unless specifically required due to a business or operational need. Most documents labelled under the previous system can retain their existing labels, provided staff are aware of the appropriate handling requirements.

2.5 Information Management (IM) Framework

A key initiative of the *NSW Government ICT Strategy* is the development of an Information Management (IM) Framework to support the way government administers and uses data and information.

The IM Framework is a set of standards, policies, guidelines and procedures that enable data and information to be managed in a secure, structured and consistent manner.

It ensures that data and information can be appropriately shared or re-used by agencies, individual public sector staff, the community or industry for better services, improved performance management and a more productive public sector.

The Guidelines form part of the IM Framework.

Appendix B highlights the operational outcomes supported by good information security practices, aligned with the IM Framework.

2.6 Related guidance

The Guidelines should be read with other guidance on classification, labelling and handling.

NSW guidance

NSW Government Digital Information Security Policy (DISP)

Agency specific policies and procedures for labelling, classifying and handling sensitive information

Related NSW legal and regulatory requirements (identified in **Appendices C** and **D**)

Australian Government PSPF guidance

Information security management guidelines – Australian Government security classification system

Information Security management guidelines – Protectively marking and handling sensitive and security classified information

Protective security governance guidelines – Business impact levels

Related Commonwealth legal and regulatory requirements

Details of these and other policies, guidelines and legislation affecting the Guidelines can be found at **Appendix C**.

2.7 Guideline revision

The Guidelines will be reviewed in July 2016 or earlier in response to post-implementation feedback, changes to the Australian Government system or when the need for new DLMs has been identified.

2.8 New DLM provision

In normal circumstances agencies **must not** create their own DLMs, security classifications or caveats. Under the Guidelines, new DLMs proposed by agencies will be considered by the Information Security Steering Group when the following conditions are met:

1. there is a specific agency need
2. there is no approved DLM which is appropriate for use

The Information Security Steering Group is made up of cluster representatives from members of the Information Security Community of Practice, which was established under the *NSW Government Digital Information Security Policy*.

This Steering Group endorses the creation of new DLMs, for which the ICT Leadership Group gives final approval. New DLMs have the same minimum control requirements for preparation and handling as those under any **Sensitive** label and can be modified by the Steering Group.

The Guidelines do not prevent agencies, on the basis of internal processes, policies and procedures, using other agency-specific markers in conjunction with the DLMs outlined in the Guidelines – for example, in round brackets after a DLM. Agency-specific markers provide additional information specific to the agency in question and should only be used in conjunction with approved DLMs and/or security classifications.

3. Introduction: protective markings

3.1 What are protective markings?

Protective markings are used to ensure the confidentiality of certain sensitive information. Information is only to be protectively marked if its compromise could damage the state or national interest, organisations or individuals, or if it requires protection under NSW or Commonwealth legislation. There are three categories of protective markings: dissemination limiting markers (DLMs), security classifications, and caveats.

The Australian Government System includes 5 DLMs:

- **For Official Use Only (FOUO)**
- **Sensitive**
- **Sensitive: Personal**
- **Sensitive: Legal**
- **Sensitive: Cabinet**

The NSW Government system includes a further four:

- **Sensitive: NSW Government**
- **Sensitive: NSW Cabinet**
- **Sensitive: Law Enforcement**
- **Sensitive: Health Information**

The NSW Government security classification system aligns with the Australian Government system, which includes four classifications:

- **PROTECTED**
- **CONFIDENTIAL**
- **SECRET**
- **TOP SECRET**

In some circumstances, information may bear a security caveat in addition to a security classification or label. The Australian Government system identifies seven categories of caveats:

- **codewords**
- **source codewords**
- **eyes only**
- **Australian Government access only**

- **releasable to**
- **special handling caveats**
- **accountable material**

Each protective marking carries with it certain limitation for dissemination and requirements for handling.

Detailed explanations of each of these categories of protective markings can be found in sections 3, 4 and 5.

3.2 What should be protectively marked?

There are two types of official information held by the NSW Government:

- information that does not need increased security
- information that needs increased security to protect its confidentiality

Most official information does not need increased security and may be marked **UNCLASSIFIED** or left unmarked. This should be the default position for newly created material, unless there is a specific need to protect the confidentiality of the information.

Information only requires increased security to protect its confidentiality if its compromise could damage national/state interest, organisations or individuals, or requires protection under NSW or Commonwealth legislation—including HRIPA and PIPPA.

Information which needs increased protection is to be either security classified and identified by a protective marking showing the level and protection required, assigned a dissemination limiting marker (DLM) or, when appropriate, assigned a caveat.

Protective markings can be applied to information in any format, medium or resource. This includes, but is not limited to, paper files or documents, digital files or documents, information assets, datasets, infrastructure, records management systems, magnetic or optical media, microforms, databases, software applications, hardware and physical assets.

3.3 Who applies protective markings?

The person responsible for preparing the information or for actioning information produced outside of the NSW Government or Australian Government determines the protective marking. This could be the “originator”, “information owner” or “risk owner”.

Agencies are to advise all employees, including contractors, on the proper use of the classification, labelling and handling system.

For protectively marked material, agencies should identify the custodian of the information and both internal and external parties that have a legitimate need to use the information.

Appendix G, Information Classification and Handling Worksheet, provides a template for identifying the parties involved with, or responsible for, the information throughout each phase of the information lifecycle.

3.4 When are protective markings applied?

When 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 it is to be given a protective marking in accordance with the Guidelines.

Information received from external sources should be evaluated upon receipt and protectively marked in accordance with the Guidelines.

An agency sending sensitive information to another government agency must label the information in accordance with the Guidelines. Information Custodians (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.

Protectively-marked information which is received from another government agency should be handled in accordance with the Guidelines and the PSPF as appropriate.

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

3.5 Agency policy and procedures for classification, labelling and handling

Under the *NSW Government Digital Information Security Policy* (DISP), agencies must have an internal information security policy which may include agency-specific procedures for classifying, labelling and handling sensitive information. Agency information classification policies must be consistent with the DISP, the Guidelines and relevant parts of the PSPF as required.

Agencies are encouraged to engage internal stakeholders to identify the stakeholders' needs for protecting sensitive information and jointly develop classification, labelling and handling procedures that meet the agency's need.

Agency policies 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

Agencies must determine specific events or dates for declassification on the basis of an assessment of 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 ensure principles of good information security practice are applied:

- sensitive information should only be released to organisations and individuals with a demonstrated need to know
- information is to be stored and processed away from public access
- the removal of information from agency premises is on the basis of identified need
- disposal of information is by secure means
- the transmission and transfer of information is by means which deter unauthorised access

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

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

Appendix E provides the handling principles for Dissemination Limiting Markers (DLM) with a common baseline approach of minimum controls for **Sensitive** information and guidance for additional controls under other DLMs.

3.6 Receiving Australian Government information

The Commonwealth requires that NSW Government agencies receiving Australian Government security classified information comply with the procedures set out in the PSPF regarding the application, removal, transfer, receipt and destruction of that information. This includes security vetting requirements outlined in the *Australian Government Personnel Security Protocol*.

Appendix F provides guidance regarding Australian Government handling requirements for security classified information.

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 set out in the Guidelines.

3.7 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 – when the consequences of information being compromised warrant the expense of increased protection.

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 employees or receiving agencies

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

3.8 Handling protectively marked information

The Guidelines set out minimum control and handling requirements for DLMs, and additional guidance is provided by the PSPF in *Information security management guidelines – Protectively marking and handling sensitive and security classified information.*

Where there is potential ambiguity in interpreting the control or handling requirements in the Guidelines, refer to principles outlined in the DISP, in particular the need to take a riskbased approach.

Minimum controls and handling requirements for material marked with a DLM and security classified material are outlined in **Appendices E** and **F** respectively. The Australian Government *Information security management guidelines – protectively marking and handling sensitive and security classified information* should be consulted.

Appendix B highlights the operational outcomes supported by good information security practices, aligned with the NSW Information Management Framework. It should be used in

conjunction with **Appendix G** in order to identify the parties involved with, or responsible for, the information throughout each phase of the information lifecycle.

3.9 Choosing a protective marking

Business impact levels (BIL) should be considered when determining if information requires a security classification. More information on BILs can be found in section 4.1 of the Guidelines, **Appendix H**, and in the Australian Government *Protective security governance guidelines – Business impact levels*.

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

4. Dissemination Limiting Markers

DLMs are used where disclosure may be limited or prohibited by legislation, or where information may otherwise require special handling. Most DLMs can be used on their own, or in conjunction with a security classification. The exception is **For Official Use Only** (**FOUO**), which may only be used with **UNCLASSIFIED** information.

The presence or absence of a protective marking will not affect a document's status under GIPA, PPIPA and HRIPA.

GIPA mandates an open, accountable, transparent approach to proactive information disclosure for NSW Government. GIPA helps to ensure that access to government information is restricted only when there is an overriding public interest against disclosure.

The 'public interest' test is the principle underpinning the procedures outlined in GIPA. Sections 12 to 15 of the GIPA Act outline public interest considerations for the disclosure of information.

4.1 For Official Use Only

For Official Use Only (**FOUO**) may be used with unclassified information only, when its compromise may cause limited damage to the national or state interest, organisations or individuals.

FOUO is typically applied to information produced by Commonwealth agencies, or to information that has Australian Government business impact implication. Sensitive information produced by NSW Government agencies that does not pose a security risk according to the NSW Government Business Impact Levels (see **Appendix H**) will typically be labelled **Sensitive: NSW Government**, not **FOUO**.

For guidance on the handling of material labelled **FOUO** – including creation and storage, dissemination and use, and archiving and disposal – see **Appendix E**.

4.2 Sensitive

Sensitive may be used with security classified or unclassified information:

- where the secrecy provisions of enactments may apply, or
- the disclosure of which may be limited or prohibited under legislation

All information labelled **Sensitive** should be handled according to the minimum controls, for which guidance can be found at **Appendix E**.

4.3 Sensitive: Personal

Sensitive: Personal may be used with security classified or unclassified information that contains attributes of personal information as defined in PPIPA.

For guidance on the handling of material labelled **Sensitive: Personal** – including creation and storage, dissemination and use, and archiving and disposal – see **Appendix E**.

4.4 Sensitive: Legal

Sensitive: Legal may be used for any information that may be subject to legal professional privilege.

For guidance on the handling of material labelled **Sensitive Legal** – including creation and storage, dissemination and use, and archiving and disposal – see **Appendix E**.

4.5 Sensitive: Cabinet

Sensitive: Cabinet is to be applied to *Australian Government Cabinet* information including:

- any document including but not limited to business lists, minutes, submissions, memoranda and matters without submission that is or has been:
  - submitted or proposed to be submitted to Cabinet
  - official records of Cabinet
- any other information that would reveal:
  - the deliberations or decisions of Cabinet
  - matters submitted, or proposed to be submitted to Cabinet

Any use of the DLM **Sensitive: Cabinet** is to be accompanied by a security classification protective marker of at least **PROTECTED** level.

Sensitive: Cabinet may also be denoted as **Sensitive: Cabinet (Cth)** in practice.

For guidance on the handling of material labelled **Sensitive Cabinet** – including creation and storage, dissemination and use, and archiving and disposal – see **Appendix B** in accordance with its security classification protective marker.

4.6 Sensitive: NSW Cabinet

Sensitive: NSW Cabinet should be applied to sensitive *NSW Government Cabinet* documents, including:

- all official records of the NSW Government Cabinet including Cabinet agendas, Cabinet submissions, Cabinet Minutes, advice on Cabinet Minutes and Cabinet decisions
- any other information that would reveal or prejudice:
  - the deliberations or decisions of the NSW Government Cabinet or
  - the position that a particular Minister has taken or may take on a matter in the NSW Cabinet
  - drafts, copies or extracts of the above documents

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.

Sensitive: NSW Cabinet should be applied to NSW Government Cabinet documents (including draft NSW Government Cabinet documents). They must be stored securely, and access should only be on a need to know basis.

Any Cabinet documents relating to national security are to be classified accordingly.

Premier's Memorandum *M2006-08 Maintaining Confidentiality of Cabinet Documents and Other Cabinet Conventions* describes the importance of, and foundation for, the confidentiality of NSW Cabinet documents. The NSW Government Ministerial Handbook outlines handling procedures for NSW Government Cabinet documents.

If there is any inconsistency between the Guidelines and the guidance, policy or processes issued by the NSW Department of Premier and Cabinet regarding the control or handling of **Sensitive: NSW Cabinet** information, the latter prevail.

Note: In addition to the above, all controls and handling requirements for **Sensitive: NSW Government** information apply to **Sensitive: NSW Cabinet**, with several additions and modifications.

For guidance on the handling of material labelled **Sensitive: NSW Cabinet** – including creation and storage, dissemination and use, and archiving and disposal – see **Appendix E**.

4.7 Sensitive: NSW Government

The **Sensitive: NSW Government** protective marking is used when the compromise of the information could cause limited damage or damage to the NSW Government, commercial entities or members of the public. For instance, where compromise could:

- endanger individuals and/or private entities
- work substantially against state or national finances or economic and commercial interests
- substantially undermine the financial viability of major organisations
- impede the investigation or facilitate the commission of serious crime
- seriously impede the development or operation of major government policies

Information that was previously labelled as P**ROTECTED** under the previous NSW labelling system may translate to the DLM **Sensitive: NSW Government**.

Sensitive: NSW Government may also be abbreviated to **Sensitive: NSW Govt**.

Note: All control and handling requirements for **Sensitive** information apply to **Sensitive: NSW Government** information – with several additions and modifications.

For guidance on the handling of material labelled **Sensitive: NSW Government** – including creation and storage, dissemination and use, and archiving and disposal – see **Appendix E**.

4.8 Sensitive: Law Enforcement

The DLM **Sensitive: Law Enforcement** is new to this update of the Guidelines. It should be applied by law enforcement agencies and is to be used for Law Enforcement activities.

It denotes that the information was compiled for law enforcement purposes and should be afforded appropriate security in order to protect certain legitimate Government interest, including enforcement proceedings, the right of a person to a fair trial, policing and community safety practices, proprietary information or to protect a confidential source.

The presence or absence of a **Sensitive: Law Enforcement** protective marking 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.

The information that may fall under these activities may include:

- law enforcement activities as defined by specific Acts outlined in **Appendix D**
- multijurisdictional operational law enforcement activity
- information relating to the security of the state or a national security matter
- information relative to law enforcement methodology

- identity of a confidential source, including an individual or private institution that furnished information on a confidential basis
- information furnished by a confidential source
- technical diagrams, drawings, schematics for law enforcement technology and architecture where disclosure would jeopardise investigations and hamper law enforcement activities
- techniques and procedures for law enforcement investigations or prosecutions
- 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 referred to in **Appendix D**. In general terms, those permitted uses are for law enforcement purposes, such as the investigation and prosecution of criminal offences.

Sensitive: Legal and **Sensitive: Law Enforcement** DLMs should not be confused. **Sensitive: Legal** should be used to protect legal professional privilege under the advice of legal professionals. **Sensitive: Law Enforcement** should only be used by law enforcement agencies for law enforcement purposes and for information that needs to remain strictly confidential.

The DLM **Sensitive: Law Enforcement** may be used in conjunction with a security classification depending on the business impact level as determined by referring to the Business Impact Level Matrix at **Appendix H**. Law enforcement information that was labelled **PROTECTED** under the previous NSW labelling systems may translate to the DLM **Sensitive: Law Enforcement** without a security classification.

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.

Information with a DLM of **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.

Note: All control and handling requirements for **Sensitive** information apply to **Sensitive: Law Enforcement information** with several additions and modifications.

For guidance on the handling of material labelled **Sensitive: Law Enforcement** – including creation and storage, dissemination and use, and archiving and disposal – see **Appendix E**.

4.9 Sensitive: Health Information

The DLM **Sensitive: Health Information** is new to this update of the Guidelines.

Sensitive: Health Information should be applied to health information as defined by the *Health Records and Information Privacy Act 2002* (NSW) section 6 definition of "health information".

Agency internal operational policy and procedures are to be developed to help manage specific labelling and handling requirements of Health Information that the agency is dealing with. The following considerations are to be taken into account:

- Health Sector agencies are to understand their corresponding obligation in dealing with Health information defined in HRIPA and comply to all relevant NSW Health published policy and guidelines.
- Non-Health Sector agencies are to understand the differences between Health Information as defined in HRIPA and Personal Information defined in PPIPA.
- Agencies need to understand the usages of both Health Information and Personal Information in the context of the agency's business activities and select the appropriate **Sensitive: Health Information** or **Sensitive: Personal** label to protect them. Agencies must define the obligations in dealing with both types of information.
- When Health information is exchanged between Health Sector agencies, **Sensitive: Health Information** marking must be applied and Health Policy and Guidelines must be observed.
- In some circumstances, other legislative requirements may supersede the use of **Sensitive: Health Information** marking. For example, **Sensitive: Law Enforcement** could be used during investigation for information that might otherwise be labelled **Sensitive: Health Information**.
- When exchanging information between Health and non-Health agencies, prior exchange agreements should be established to protect information labelled **Sensitive: Health Information**.

All Health Information is to be collected and protected in accordance with HRIPA. Operational guidance for Health Information protection is provided via NSW Health Privacy Manual. Agencies are to refer NSW Health policy website for latest information and guidance (http://www.health.nsw.gov.au/policies/pages/default.aspx).

General guidance to protect Health Information is also available from ISO27799 standard.

For guidance on the handling of material labelled **Sensitive: Health Information** – including creation and storage, dissemination and use, and archiving and disposal – see **Appendix E**.

5. Security classifications

Security classifications have been the subject of a memorandum of understanding between the NSW and Australian Governments.

NSW agencies that handle information requiring security classification must manage this information in accordance with Australian Government requirements, including appropriate security clearances. Only a small number of agencies deal with information at this level.

Security classifications **PROTECTED, CONFIDENTIAL**, **SECRET** and **TOP SECRET** are to be regarded as national security classifications under the Guidelines.

Personnel who access information that is classified at a level of **PROTECTED** or above should be security-vetted.

5.1 Business impact levels (BILs)

The Australian Government *Protective security governance guidelines – Business impact levels* provides guidance for agencies so they can apply a consistent approach to assessing business impact in applying security classifications.

It is recognised that a given information risk would not necessarily have the same business impact on each party in a collaboration and agencies may have to develop their own business impact level matrix. Agency should align with **Appendix H** – *Australian Government Business Impact Levels Guidance* while developing a detailed agency BIL matrix.

National interest information is any official resource including equipment that records official information concerning Australia's:

- national security:
    - protection from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, acts of foreign interference and the protection of Australia's territorial and border integrity from serious threats ○ defence capability
- international relations, significant political and economic relations with international organisations and foreign governments
- law and governance, including:
    - interstate/ territory relations

    - law enforcement operations where compromise could hamper or make useless national crime prevention strategies or particular investigations, or endanger personal safety

- economic, scientific or technological matters vital to Australia's stability, integrity and wellbeing
- heritage or culture

Security classification is applied to national and state interest information that requires protection based on the BILs of its unauthorised disclosure or misuse. Each level of classification reflects the consequences of unauthorised disclosure and has strict handling and security clearance requirements.

The BIL scale ranges from 1 (Low/Medium impact) to 5 (catastrophic impact), with BIL levels 2, 3, 4 and 5 matching respectively to **PROTECTED**, **CONFIDENTIAL**, **SECRET** and **TOP SECRET** security classifications. Information with a BIL of 1 may be **UNCLASSIFIED** or carry a DLM such as **FOUO**. However, in some circumstances, both a DLM and a security classification will be applied.

It is not the case that an aggregation of assets with a BIL of 4 for confidentiality necessarily will be marked individually at **SECRET**. The *Australian Government information security management guideline – management of aggregated information* provides further guidance on managing aggregated data.

5.2 UNCLASSIFIED material

Most information handled by NSW Government agencies is of low sensitivity and requires only limited protection. Where the information does not require a security classification it may be marked **UNCLASSIFIED** if required by agency policy.

UNCLASSIFIED is not a protective marking or a security classification. **UNCLASSIFIED** may be used in conjunction with a DLM with a BIL of 1.

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

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

Material created on or after 1 July 2015 is regarded as unlabelled and **UNCLASSIFIED** where no protective marking is used.

5.3 PROTECTED

The **PROTECTED** security classification is used when the compromise of the information could cause damage to the Australian Government, commercial entities or members of the public. For instance, where compromise could:

- endanger individuals and private entities – the compromise of information could lead to serious harm or potentially life threatening injury to an individual
- work substantially against state or national finances or economic and commercial interests
- substantially undermine the financial viability of major organisations
- impede the investigation or facilitate the commission of serious crime
- seriously impede the development or operation of major government policies

Personnel who access information that is classified at a level of **PROTECTED** or above should be security-vetted.

Information should be labelled **PROTECTED** when compromise of the confidentiality of information could be expected to cause damage to national interest, organisations or individuals.

Examples of types of information which could cause damage and require the use of **PROTECTED** can be found in **Appendix H** with business impact level 2 (High). For relevant control and handling requirements for **PROTECTED** information, agencies are directed to the PSPF and *Information security management guidelines – Protectively marking and handling sensitive and security classified information*.

5.4 CONFIDENTIAL

Information should be labelled **CONFIDENTIAL** when compromise of the confidentiality of information could be expected to could cause significant damage corresponding to national interest, organisations or individuals with a business impact level 3 (Very High), according to the Australian Government *Protective Security Governance Guidelines – Business impact levels*.

Examples of types of information which could cause significant damage and require the use of **CONFIDENTIAL** can be found in **Appendix H**.

For relevant control and handling requirements for **CONFIDENTIAL** information agencies are directed to the PSPF and Information security management guidelines – Protectively marking and handling sensitive and security classified information.

5.5 SECRET

Information should be labelled **SECRET** when compromise of the confidentiality of information could be expected to cause serious damage corresponding national interest, organisations, or individuals with a business impact level 4 (Extreme).

Examples of types of information which could cause serious damage and require the use of **SECRET** can be found in **Appendix H**.

For relevant control and handling requirements for **SECRET** information agencies are directed to the PSPF and *Information security management guidelines – Protectively marking and handling sensitive and security classified information*.

5.6 TOP SECRET

Information should be labelled **TOP SECRET** when compromise of the confidentiality of information could be expected to could cause exceptionally grave damage corresponding to a business impact level 5 (Catastrophic).

Examples of types of information which could cause serious damage and require the use of **TOP SECRET** are in **Appendix H**.

For relevant control and handling requirements for **TOP SECRET** information agencies are directed to the PSPF and *Information security management guidelines – Protectively marking and handling sensitive and security classified information*.

For relevant control and handling requirements for **TOP SECRET** information agencies are directed to the PSPF and *Information security management guidelines – Protectively marking and handling sensitive and security classified information*.

6. Caveats

When to use caveats

Certain security classified information, most notably some national security classified information, may bear a security caveat in addition to a security classification. The caveat is a warning that the information has special requirements in addition to those indicated by the protective marking.

Caveats are not used with DLMs and are not used on their own without an accompanying security classification. Caveats should not be used extensively in NSW.

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

Modifications to wording of caveats may take place with the approval of the Information Security Steering Group.

Removing caveats

Information bearing agency-specific caveats is to be re-labelled or appropriate procedures agreed before release or transmission outside of that agency.

The prior agreement of the originating agency – in other words, the agency that originally placed the caveat on the material – is required to remove a caveat. If the originating agency will not agree to the removal of the caveat then the information cannot be released. The

requirement to obtain agreement of the originating agency to release the material cannot be the subject of a policy exception under any circumstances.

6.1 Codewords

A codeword is a word indicating that the information it covers is in a special need to know compartment.

It is often necessary to take precautions beyond those normally indicated by the security classification to protect this information. These precautions will be specified by the organisation that owns the information – for instance, those with a need to access the information will be given a special briefing first.

The codeword is chosen so that its ordinary meaning is unrelated to the subject of the information.

Few NSW Government employees outside of key agencies will have cause to use codewords.

6.2 Source codewords

A source codeword is a word or set of letters used to identify the source of certain information without revealing it to those who do not have a need to know.

6.3 Eyes Only

The **Eyes Only** (**EO**) marking indicates that access to information is restricted to certain groups or jurisdictions, or nationalities in the case of national information, for instance:

- **AUSTEO** means **Australian Eyes Only**
- **AUST/US EO** means **Australian and US Eyes Only**, and
- **NSWEO** means **New South Wales Government Eyes Only**

Any information marked **EO** cannot be passed to or accessed by those who are not listed in the marking. More information on **EO** is outlined in the PSPF.

6.4 Australian Government Access Only (AGAO)

In limited circumstances **AGAO** is used by the Department of Defence and the Australian Security Intelligence Organisation (ASIO). It means these agencies may pass information marked with the **AGAO** caveat to appropriately cleared representatives of foreign governments on exchange or long-term posting or attachment to the Australian Government.

6.5 Releasable to

The caveat **RELEASABLE TO** identifies information that has been released or is releasable to the indicated foreign countries only – for example, **REL GB**,**NZ** means that the information may be passed to the United Kingdom and New Zealand only.

RELEASABLE TO markings are to employ the appropriate two letter country codes from the *SAI Global - ISO 3166-1 Alpha 3 Codes for the representation of names of countries and their subdivisions.*

6.6 Special handling caveats

A special-handling caveat is a collection of various indicators such as operation codewords, instructions to use particular communications channels and **EXCLUSIVE FOR** (named person). This caveat is usually used only within particular need to know compartments.

There are special requirements for some caveat or codeword information. These are determined by the controlling agency and provided on a need to know basis.

6.7 Accountable Material

If strict control over access to, and movement of, particularly sensitive information is required, originators can make this information **Accountable Material**. What constitutes **Accountable Material** will vary from agency to agency, but could include budget papers, tender documents and sensitive ministerial briefing documents.

Accountable Material is subject to the following conditions:

- the caveat '**Accountable Materia**l' can be in bold print on the front cover of the material – not necessary for Cabinet documents, **TOP SECRET** information or codeword material
- it is to carry a reference and individual copy number – agencies could also consider making each page accountable by numbering (for example, page 3 of 10), and placing the document copy number on each page
- it is to carry a warning such as: not to be copied without the prior approval of the originator
- it is only to be passed by hand or safe hand – if it is passed to another person, a receipt is to be obtained
- a central register is to be maintained of all persons having access to each accountable document – this central register is separate from the movement record which forms part of the document or file.

List of Appendices

Appendix A – Glossary of Key Terms

Appendix B – Application of Information Management Stages

Appendix C – Resources

Appendix D – Legislation Reference **Sensitive: Law Enforcement**

Appendix E – Handling guidelines for Dissemination Limiting Markers

Appendix F – Handling of Security Classified Material

Appendix G – Information Classification and Handling Worksheet

Appendix H – Australian Government Business Impact Levels Guidance

7. Appendix A Glossary of Key Terms

The following glossary provides definitions for terms that are not otherwise explained in the text of the Guidelines.

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.
Clear desk policy	The term *Clear desk policy* means that items with a protective marking must be secured when unattended and their content always unobservable to people without the *Need to know*.
Damage	*Damage* referred to in these Guidelines may be financial, commercial or reputational damage to any NSW Government agency, the NSW Government, the Australian Government, or an Australian Government agency.
National security information	Official information whose compromise could affect the security of the nation. *National security information* could include information about security threats from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence, acts of foreign interference or serious organised crime, as well as the protection of Australia's borders.
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 responsible for preparing or for actioning external information is called the *Originator* (see Australian Government Security Classification System).
Owner	The term *owner* identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term *owner* does not mean that the person actually has any property rights to the asset (see ISO/IEC 27001:2005).
Risk Owner	The *Risk Owner* is the person or entity with the accountability and authority to manage a risk (see ISO/IEC 27000:2014).
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 PSPF for guidance).
Central register	A central record is to be maintained of all persons having access to any information marked TOP SECRET or *Accountable Material*. This register is separate from any movement record which forms part of the document or file (see the PSPF for guidance).
UNCLASSIFIED	Official information that is not expected to cause harm and does not require a security classification; it may be unlabelled or it may be marked *UNCLASSIFIED*. UNCLASSIFIED is not a protective marking or a security classification. This type of information represents the bulk of official information.

A glossary of related security terms can be found in the Australian Government Protective Security Policy Framework – Glossary of security terms

8. Appendix B Application of Information Management Stages

The following information management stages are aligned with the NSW Information Management Framework and interpreted in the context of information classification, labelling and handling.

Govern

Classification, labelling and handling requirements for information are determined by the strategic, operational and administrative value of information to the NSW Government agencies. Each identified information asset must be assessed for sensitivity based on its

legislative, policy, legal requirements and the impact and consequences of loss or unauthorised disclosure. This is to ensure the corresponding classification label is applied and the information is appropriately handled in a manner that protects public and government interests.

Collect

The collect stage includes both information creation and collection. The information owner with the responsibility and authority must be determined when information is created and collected. Information owners must assess the classification of information, using the *NSW Information and Classification Guidelines* and NSW Classification and Labelling App (http://finance.nsw.gov.au/ict/app/) as a guide. Information owners are responsible for owning information risk. When information is collected, the information owner must consider its needs and its corresponding lifespan maintenance.

Organise and Secure

Information must be organised and protected appropriately to ensure it is readily available when needed, can be reliably used, is handled and shared according to its sensitivity to prevent unauthorised access, use and disclosure. Refer to **Appendices E** and **F** for Information Handling guidance.

Use and Share

Information must be used appropriately and shared according to its classification with a pre-defined agreement. An information lifespan approach is used to help determine the corresponding classification, labelling and handling requirements throughout the lifespan in order to manage the information to serve business needs. Below is an example illustrating various organisation functions (such as function X, Y, S) and 3rd party organisations (such as org A) having information roles at their corresponding information management stages, outlined below:

Govern	*Collect*	*Organise*	*Secure*	*Use*	*Share*	*Maintain*
Function S	*Function X* *Function Y*	*Function Y*	*Function A, B, S, X, Y, Z* *External Org A*	*Function Z* *Function A* *Function B*	*Function X* *External Org A*	*Function Y*

Maintain

Information including data and records are to be kept for the minimum period as required by legislation and any relevant policy, then disposed systematically. Information maintenance can mean many things, for instance it could involve:

- information de-classification over time
- ensuring sensitive information can still be decrypted
- information on certain digital media is maintained and can still be read over time

Updating information is considered to be creating a new set of information rather than information maintenance. Information under this context is treated as static information. Other guidance for the disposal of information can be found in **Appendix E**.

9. Appendix C Resources

The following table provides a list of other resources which may influence information security classification and labelling procedures.

References
Australian Government Protective Security Policy Framework (PSPF) – documents map
Information security management guidelines – Australian Government security classification system
Information security management guidelines – Protectively marking and handling sensitive and security classified informatio n
Government informatio n security management guideline – management of aggregated information
Australian Government Protective Security Policy Framework – Securing Government business
Protective Security Governance Guidelines – Business Impact Levels
Australian Government Personnel Security Protocol
Physical security management guidelines
Information Security Manual
Privacy Act 1988 (Australian Government)
NSW Digital Information Security Policy
Health Records and Information Privacy Act 2002 (NSW)
Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA)
Government Information (Public Access) Act 2009 (NSW) (GIPA)
State Records Act 1998 (NSW)
Court Information Act 2010 (NSW)
Public Health Services: Patient/Client Records, General Retention and Disposal Authority (GDA17)
NSW Guide to Labelling Sensitive Information 2011 (previous system in NSW)
NSW Government ICT Strategy
Cabinet Conventions: NSW Practice
M2006-08 Maintaining Confidentiality of Cabinet Documents and Other Cabinet Conventions
M2007-13 Release of NSW Government Security Sensitive Information to Third Parties

M2008-17 NSW Policy and Guidelines for Protecting National Security Information
Ministerial Handbook

10. Appendix D – Legislation Reference Sensitive: Law Enforcement

For multi-jurisdictional and Commonwealth matters the legislation may include but is not limited to:

- Australian Crime Commission Establishment Act 2002 (Australian Government)
- Surveillance Devices Act 2004 (Australian Government)
- Taxation Administration Act 1953 (Australian Government) s. 355
- Telecommunications (Interception and Access) Act 1979 (Australian Government) s.178, 179 and 180

For NSW law enforcement, matters the legislation may include but is not limited to:

- Law Enforcement Powers and Responsibilities Act 2002 (NSW) (LEPRA)
- Police Act 1990 (NSW)
- Police Regulation 2008 (NSW)

Additional legislative restrictions may also apply to the provision of access to information and the way it must be handled. Access must be in accordance with (but not limited to):

- Child Protection (Offenders registration) Act 2000 (NSW)
- Crime Commission Act 2012 (NSW)
- Crimes Act 1900 (NSW)
- Director of Public Prosecutions Act 1986 (NSW)
- Drug Misuse and Trafficking Act 1985 (NSW)
- Firearms Act 1996 (NSW)
- Law Enforcement (Controlled Operations) Act 1997 (NSW),
- Law Enforcement and National Security (Assumed Identities) Act 2010 (NSW)
- Ombudsman Act 1974 (NSW)
- Passenger Transport Regulation 2007 (NSW)
- Police Integrity Commission Act 1996 (NSW)
- Public Interest Disclosures Act 1994 (NSW)
- State Emergency and Rescue Management Act 1989 (NSW)

- Surveillance Devices Act 2007 (NSW)
- Surveillance Devices Amendment (Police Body-Worn Video) Act 2014 (NSW)
- Witness Protection Act 1995 (NSW)

11. Appendix E – Handling Guidelines for Dissemination Limiting Markers

Creation and Storage

		Sensitive (Minimum Controls)	Sensitive: Personal	Sensitive: NSW Government	Sensitive: NSW Cabinet	Sensitive: Legal	Sensitive: Health Information	Sensitive: Law Enforcement
Creation and Storage	**Secure** **Organize** **Collect** **Govern**	• The controls applied for the storage of any information marked **Sensitive** must ensure that the information remains confidential and is available to authorised individuals when it is needed ("need to know"). • Information should be created and stored in a manner that preserves the integrity of the source information. These requirements apply to both physical and electronic information and controls may include perimeter controls, encryption, two factor authentication and other relevant security controls. • Security controls must be applied to satisfy Legislative, Regulatory, Policy and Legal (e.g. Legal Professional Privilege) requirements. • The controls applied must meet Minimum Standards for Marking, Filing and Handling sensitive information including the following: • Marking: centre of top and bottom of each page; markings should be in bold text and a minimum of 5mm high (preferably red stamp); the label on a file cover or container must be at least equal to the label on the most sensitive item in the file or container; paragraph markings, where adopted, should appear in a consistent position such as at the; end of each paragraph (refer to the PSPF for guidance on applying paragraph markings); and electronic and other documents should include their sensitivity label in their metadata as appropriate. • Numbering: page and/or paragraph numbering is desirable; filing and media labels; front and back file covers and media labels to be marked Sensitive in large letters; and an agency may reserve specific colours for file covers and media labels covering sensitive items.	**Sensitive** (Minimum Controls) plus: • Personal information must only be collated for authorised purposes, as defined in PPIPA. • Personal information must be kept in a designated location physically and/or electronically, and its access limited to only authorised personnel.	**Sensitive** (Minimum Controls) must be applied.	**Sensitive** (Minimum Controls) plus: The following additional legislations, policy, guidelines are to be observed in handling NSW Cabinet and related materials: • Premier's Memorandum M2006-08, M2015-03 • Cabinet documents and other state papers – 2011 General State election Agencies are to refer to NSW Ministerial Handbook for specific guidance Accountability of **Sensitive: NSW Cabinet** document is required to be maintained at all times. Agency specific cabinet process, policies and guidelines to ensure agency NSW Cabinet processes are put in place to securely handle NSW Cabinet information	**Sensitive** (Minimum Controls) plus: The following are to be observed in handling **Sensitive: Legal** materials: • Legal Professional Act 2004 • Legal Professional Regulation 2005 • Evidence Act 1995 • Criminal Procedure Act 1986 • New South Wales Barristers' Rules As a client, all legal advice provided by legal professional and/or specified by legal professional subject to Legal Professional Privilege are required to be marked with **Sensitive: Legal**. Non-disclosure of **Sensitive: Legal** documents must be strictly observed to preserve Client Privilege.	**Sensitive** (Minimum Controls) and **Sensitive: Personal** controls plus: • Sensitive health information should be collected in accordance with the Health Records and Information Privacy Act 2002. Information can only be collected if the purpose of collecting is directly related to what the agency does and the collection is necessary for those purposes. Refer to Statutory Guidelines and Health Privacy Principles published on Information and Privacy Commission web site. (http://www.ipc.nsw.gov.au/hripact) NSW Health Privacy Manual can also be used for operational guidance in dealing with Health Information for health related services. • A secure physical and electronic environment should be maintained for all data held on computer systems. • All paper records containing personal health information should be kept in lockable storage or secure access areas when not in use. Basic precautions such as not storing records containing personal health information in a public area should not be overlooked. • Care should be taken not to leave documents containing personal health information on work benches or anywhere they may be visible to unauthorised people. More detailed operational guidance is available at NSW Health policy website. (http://www.health.nsw.gov.au/policies/pages/default.aspx)	**Sensitive** (Minimum Controls) plus: • **Sensitive: Law Enforcement** DLM can be used in conjunction with Australian Government Security Classification system. The corresponding handling requirements are specified in the *ISM Guidelines – Protectively Marking and Handling Sensitive and Security Classified Information* document. • Where there is other sensitive information such as personal or health information, it is necessary to comply with the appropriate legislative requirements as well as the corresponding requirements stated in the Guidelines.

Dissemination and use

		Sensitive (Minimum Controls)	Sensitive: Personal	Sensitive: NSW Government	Sensitive: NSW Cabinet	Sensitive: Legal	Sensitive: Health Information	Sensitive: Law Enforcement
Dissemination and use	**Secure** **Maintain** **Use** **Share**	• For information classified with a DLM, agencies are to implement processes that establish rules for the disclosure of this type of information. Dissemination of information must be for authorised purposes. • The information owner at each agency, has overall accountability for access that is provided, is to determine both internal and external parties requiring access to the information, and the business reason for this access. • Authorisation should be explicitly sought or an authorisation control is to be embedded into the relevant business processes. • Controls, including physical and logical controls, must be applied to protect information during use, to preserve confidentiality, integrity and availability. • DLM marked information cannot be removed from Agency premises, unless specifically authorised. • The controls required for transferring DLM marked information will be dependent on the volume of information being transferred (i.e. one subject or multiple subjects) and the destination of the information (i.e. to the subject or to another party). Where electronic information is being transferred either physically or from system to system, authentication, access control, "not in clear text", and audit trail should be considered as basic controls. • Copying, faxing, scanning and printing should only be carried out where minimum security requirements are met. • Clear desk/clear screen policies are to be implemented.	**Sensitive** (Minimum Controls) plus: • Personal information must only be used for authorised purposes, as defined in PPIPA. • **Sensitive: Personal** information that can cause damage to individuals or a group of people requires "security classification." When security classification is assigned, the relevant controls must be applied, as detailed in the corresponding security classification in this guideline. • Duplication of information by copying, faxing, scanning and printing should be reduced to minimal. Each piece of duplicated information (whether in electronic or physical form) is required to be equally protected as the original. This also applies to information sourced from protected systems.	**Sensitive** (Minimum Controls) plus: • Controls should be appropriately applied to ensure the physical security of information in transit. Where electronic information is being transferred either physically or from system to system, encryption should be considered as an appropriate control. • Consideration must be given to whether it is appropriate to remove documents or files from the Agency premises and the Government Guide Working Away from the Office provides further assistance.	**Sensitive** (Minimum Controls) plus: • Agency must ensure Cabinet and related materials (incl. work-inprogress, drafts) are secured at all stages including preparation stage. • Access to NSW Cabinet related information, including during preparation of a submission, is to be granted on a "need to know" basis. This includes conversation. • The responsibility for securing **Sensitive: NSW Cabinet** information must be explicitly acknowledged by the recipient during transfer. • An audit trail of access to Cabinet information in both physical and electronic form must be maintained. • **Sensitive: NSW Cabinet** materials are not to be copied to local hard disk or any removable media storage once lodged in the eCabinet system. • Cabinet documents 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. • Accessing official cabinet records electronically is governed by strict protocols to ensure confidentiality and security. Access may only be granted by the Cabinet Secretariat and may not be transferred.	**Sensitive** (Minimum Controls) plus: • The Agency is required to make all staff aware of the nature of **Sensitive: Legal** and the importance of preserving Client Privilege. • **Sensitive: Legal** documents should always be kept confidential. If disseminating **Sensitive: Legal** document is necessary, the recipient of the document is to be explicitly notified the importance of maintaining confidentiality to preserve agency's Client Privilege. • For example: Legal advice must be kept confidential throughout the agency in order to preserve the client's rights to claim Client Privilege.	**Sensitive** (Minimum Controls) plus: • No personal health information, including admission and discharge dates, should be given over the phone unless it has been established that the caller has legitimate grounds to access the information and can give proof of identity. • Cryptographic controls should be deployed and managed as directed by the regulations governing such usage. • Access to NSW Health networks and resources shall be granted to only those entities who agree on consent of monitoring. • Audit logs should be kept for the appropriate retention period to assist in future audit and access control monitoring, these logs should be protected from any accidental or deliberate modification. Section "Using and disclosing personal health information (HPP10 & HPP11)" from NSW Health Privacy Manual should be observed. Latest policies and guidelines are available from NSW Health policy website (http://www.health.nsw.gov.au/policies/pages/default.aspx)	**Sensitive** (Minimum Controls) plus: • **Sensitive : Law Enforcement** labelled information is not to be released by an agency to a third party (including other agencies) without the written approval of the law enforcement agency that applies the **Sensitive: Law Enforcement** Label to create the sensitive law enforcement information. This includes information sought through various freedom of information legislation or court subpoenas. • Manual and electronic transfer within a single physical location • Single sealed opaque envelope and passed by hand or may be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between members of staff with the need to know and there is no opportunity for any unauthorised person to view the information • Manual and electronic transfer between establishments • single sealed opaque envelope that does not give any indication of the classification AND delivered direct, by hand, by an authorised messenger, or • double, sealed envelope AND delivered securely by an overnight courier that is endorsed in line with the agency security plan using the safe hand level of service. If sensitive law enforcement information is shared externally and not through a secure or accredited network then consideration should be given to the use of appropriate encryption methods if the sensitivity of the information warrants this level of protection.

Archiving and Disposal

		Sensitive (Minimum Controls)	Sensitive: Personal	Sensitive: NSW Government	Sensitive: NSW Cabinet	Sensitive: Legal	Sensitive: Health Information	Sensitive: Law Enforcement
Archiving and Disposal	**Secure** **Maintain** **Govern**	• Information labelled **Sensitive** information must be disposed of in a manner which ensures the information is not recoverable or accessible by an unauthorised individual. This includes both physical information and information held on electronic media, including information being stored and information in transit. • 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 State Records' website for further information on retention and disposal authorities and guidance on information/record retention, disposal, and archiving. • Sensitive information in paper form should be disposed of by shredding and pulping. Where large volumes of paper are involved, specialised services for the secure disposal of confidential material should be used. • Sensitive information in electronic format should undergo sanitisation (see the Australian Government ISM for guidance). • Records should be destroyed in ways that ensure that they cannot be recovered or reconstituted. Destruction should be documented and contractors used for destruction should provide certificates of destruction. • Records required as State archives in current retention and disposal authorities should be transferred to State Records NSW as appropriate.	**Sensitive** (Minimum Controls) plus: Personal information is subject to archive requirements as defined in PPIPA. Personal information must be disposed of in a manner which ensures the information is not recoverable or accessible by an unauthorised individual. This includes both physical information and information held on electronic media, including information being stored and information in transit.	**Sensitive** (Minimum Controls) must be applied.	**Sensitive** (Minimum Controls) plus: • All Non-required records and materials used in drafting stage are to be accounted for and securely disposed after a submission is made. • Detail audit requirements for the whole cabinet process are required to be determined and implemented.	**Sensitive** (Minimum Controls) must be applied.	**Sensitive** (Minimum Controls) plus: General guidance could also be sought from AS/ISO27799 Information security management in health using ISO/IEC 27002	**Sensitive** (Minimum Controls) plus: If 'Accountable Material': under supervision of two officers who must supervise the removal of the material to the point of destruction, ensure that destruction is complete and sign a certificate of destruction.

Secure destruction services are available under NSW Government Waste Management (see http://www.procurepoint.nsw.gov.au/contracts/c9698-0)

Further guidance and requirements for the use of information and information technology can be found in the Government Guide **Working Away from the Office** and the **Information Security Manual**

Cabinet information in these guidelines includes any form of information that contains Cabinet related information. These include any form of documents in both physical and electronic forms, visual and audio forms such as, but not limited to, videos, pictorial images, diagrams, charts for visual information and analogue tapes, digital recordings, verbal conversations for audio information, etc. For GIPA purposes, Cabinet Information is defined in GIPA schedule 3

Sensitive: NSW Cabinet materials are Cabinet Information labelled with **Sensitive: NSW Cabinet** label

12. Appendix F – Handling of Security Classified Material

TOP SECRET										
PREPARATION AND HANDLING			REMOVAL AND AUDITING		COPYING, STORAGE & DESTRUCTION			PHYSICAL TRANSFER	
SECURE	ORGANISE	USE	SECURE	MAINTAIN	SECURE	USE	MAINTAIN	SECURE	SHARE

Marking Centre of top and bottom of each page. Markings are to be in capitals, bold text and a minimum of 5 mm high—preferably in red. Paragraph classifications should appear in a consistent position in the left margin adjacent to the first letter of the paragraph. **Numbering** Page numbering essential. Copy numbering essential. **Filing** Distinctive file cover, standard colour is post office red. **Classified document register** Record is to be kept of incoming and outgoing material. All incoming documents are to be placed immediately in an appropriate file cover. 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 State Records NSW website for further information on retention and disposal authorities and guidance on information/record retention, disposal, and archiving. TOP SECRET material should be maintained preferably in a separate registry, staffed only by persons authorised to handle such material. If the volume of work does not justify a separate Top Secret registry an appropriate officer is to be authorised to carry out Top Secret registry duties. **Disclosure or access** Security clearance to Negative Vetting 2 and a 'need-to-know'. Only in accordance with legislative and administrative requirements.	**Removal of documents or files** Basis of real need, e.g., meeting. Is to be in personal custody of individual and kept in SCECendorsed container e.g., briefcase, pouch, bag. Removal is to be authorised by the manager (or equivalent) responsible for the resource. Advice from ASA should be sought when removing for business purposes such as meeting or conference. Alternative arrangements (e.g., send ahead by SAFEHAND) should be considered. A written record of removal of TOP SECRET material is to be maintained. TOP SECRET material is not to be the subject of home-based work. **Audits** It is essential to conduct audits at irregular intervals. People nominated to conduct spot checks are required to sight documents and acknowledge this in writing. This process should be carried out in conjunction with the owner of the information or resource.	**Copying** Is to be copy-numbered. People authorising the copying of TOP SECRET information are to record in the file bearing the original, details of the number of copies made and their distribution. To be kept to a minimum in keeping with operational requirements. Any safeguards imposed by the originating authority are to be strictly observed. **Physical safe-keeping—minimum standards** Clear desk policy. Agencies are to refer to the PSPF—*Australian Government physical security management guidelines—Security zones and risk mitigation control measures.* **Disposal** Unless required for Archival purposes, TOP SECRET material should be destroyed as soon as possible once it is no longer required for operational purposes. ***Paper waste only*** Only appropriate SCEC-endorsed and ASIO approved equipment and systems are to be used. As it is 'Accountable Material', under supervision of two officers cleared to the appropriate level that are to supervise the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate. ***ICT media and equipment*** Is to undergo sanitisation or destruction in accordance with ISM.	**Within a single physical location** Single opaque envelope indicating the classification of the information AND receipt required AND one of the following: either passed by hand between people who have the appropriate clearance and 'need-to-know', OR placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger. May also be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate clearance and 'need-to-know' and there is no opportunity for any unauthorised person to view the information. **Transfer between establishments within Australia** Double-enveloping required AND receipt required AND one of the following: placed in an approved briefcase, satchel or pouch and delivered direct by an authorised messenger, OR delivered by SCEC-endorsed safe hand courier, OR delivered by an agency specific alternative approved by ASIO. **Outside Australia** Double enveloping required AND receipt required AND DFAT courier service required.

SECRET			
PREPARATION AND HANDLING	**REMOVAL AND AUDITING**	**COPYING, STORAGE & DESTRUCTION**	**PHYSICAL TRANSFER**

SECURE	ORGANISE	USE	SECURE	MAINTAIN	SECURE	USE	MAINTAIN	SECURE	SHARE
Marking Centre of top and bottom of each page. Markings are to be in capitals, bold text and minimum of 5 mm high (preferably red). Paragraph classifications should appear in a consistent position in the left margin adjacent to the first letter of the paragraph. **Numbering** Page and numbering essential. Serial number if in series. **Filing** Distinctive file cover, standard colour is salmon pink. **Classified document register** Record should be kept of incoming and outgoing material. All incoming documents are to be placed immediately in an appropriate file cover. If declared by the originator as Accountable Document or Material, it is to have both a reference and copy number. 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 State Records NSW website for further information on retention and disposal authorities and guidance on information/record retention, disposal, and archiving. **Disclosure or access** Security clearance to Negative Vetting 1 or above and 'need-toknow'. Only in accordance with legislative and administrative requirements.			**Removal of documents or files** Basis of real need, e.g., meeting. Is to be in personal custody of individual and kept in SCECendorsed container e.g., briefcase, pouch, bag. Removal is to be authorised by the manager (or equivalent) responsible for the resource. For home-based work, agencies are to refer to the *Australian Government physical security management guideline—Working away from the office* (to be developed). A written record of removal is to be maintained. **Audits** Where a register is maintained, audits should be conducted at irregular intervals. Personnel nominated to conduct spot checks are required to sight documents and acknowledge this in writing. This process should be carried out in conjunction with the owner of the information or resource.			**Copying** May be prohibited by originator. To be kept to a minimum in keeping with operational requirements. **Physical safe-keeping—minimum standards** Clear desk policy. Agencies are to refer to the *PSPF—Australian Government physical security management guidelines—Security zones and risk* mitigation *control measures*. **Destruction** ***Paper waste only*** Only appropriate SCEC-approved equipment and ASIO approved systems are to be used. If Accountable Material, under supervision of two officers cleared to the appropriate level who is to supervise the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate. ***ICT media and equipment*** Is to undergo sanitisation or destruction in accordance with ISM.			**Within a single physical location** Single opaque envelope indicating the classification, receipt at discretion of originator, and either: passed by hand between people who have the appropriate security clearance and 'needto-know', OR placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger. May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate clearance and 'need-to-know' and there is no opportunity for any unauthorised person to view the information. **Transfer between establishments within Australia** Double-enveloping required AND receipt required AND one of the following: placed in an approved briefcase, satchel or pouch and delivered direct by an authorised messenger OR delivered by SCEC-endorsed overnight courier OR delivered by an agency specific alternative approved by ASIO. **Outside Australia** Double enveloping required, receipt required and carriage by DFAT courier service or other authorised officers required.	

CONFIDENTIAL									
PREPARATION AND HANDLING			REMOVAL AND AUDITING		COPYING, STORAGE & DESTRUCTION			PHYSICAL TRANSFER	
SECURE	ORGANISE	USE	SECURE	MAINTAIN	SECURE	USE	MAINTAIN	SECURE	SHARE

Marking

Centre of top and bottom of each page.

Markings are to be in capitals, bold text and a minimum of 5 mm high (preferably red).

Paragraph classifications should appear in a consistent position in the left margin adjacent to the first letter of the paragraph.

Numbering

Page or paragraph numbering desirable.

Filing

Distinctive file cover, standard colour is green.

Classified document register

It is good security practice to keep a record of incoming and outgoing 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. See State Records NSW website for further information on retention and disposal authorities and guidance on information/record retention, disposal, and archiving. If declared by the originator as Accountable Document or Material, it is to have both a reference and copy number.

Disclosure or access

Security clearance to Negative Vetting 1 or above and 'need-to-know'.

Only in accordance with legislative and administrative requirements.

Removal of documents or files

Basis of real need, e.g., meeting.

Is to be in personal custody of individual and kept in SCEC-endorsed container e.g., briefcase, pouch, bag.

Removal is to be authorised by the manager (or equivalent) responsible for the resource.

For home-based work, refer to the *Australian Government physical security management guidelines—Working away from the office* (to be developed).

Audits

It is good security practice to implement spot checks of information at this level.

Copying

May be prohibited by originator.

To be kept to a minimum in keeping with operational requirements.

Physical safe-keeping—minimum standards

Clear desk policy.

Agencies are to refer to the *PSPF—Australian Government physical security management guidelines—Security zones and risk mitigation control measures*.

Destruction

Paper waste only

Only appropriate SCEC-approved or ASIO approved equipment and systems are to be used.

If Accountable Material, under supervision of two officers cleared to the appropriate level who are to supervise the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate.

ICT media and equipment

Is to undergo sanitisation or destruction in accordance with ISM.

Within a single physical location

Single opaque envelope indicating the classification, receipt at discretion of originator, and either:

passed by hand between people who have the appropriate security clearance and 'needto-know', OR

placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger.

May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate clearance and 'need-to-know' and there is no opportunity for any unauthorised person to view the information. **Transfer between establishments within Australia EITHER:**

Single opaque envelope that does not give any indication of the classification AND placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger AND receipt required

OR

Double enveloping AND receipt required AND delivered either by SCEC-endorsed overnight courier or by an agency specific alternative approved by ASIO.

Outside Australia

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

PROTECTED									
PREPARATION AND HANDLING			REMOVAL AND AUDITING		COPYING, STORAGE & DESTRUCTION			PHYSICAL TRANSFER	
SECURE	ORGANISE	USE	SECURE	MAINTAIN	SECURE	USE	MAINTAIN	SECURE	SHARE

PREPARATION AND HANDLING	REMOVAL AND AUDITING	COPYING, STORAGE AND DESTRUCTION	PHYSICAL TRANSFER
Marking Centre of top and bottom of each page. Markings are to be in capitals, bold text and a minimum of 5 mm high (preferably red). Paragraph classifications, where adopted, should appear in a consistent position such as in the left margin adjacent to the first letter of the paragraph. **Numbering** Page or paragraph numbering desirable. **Filing** Distinctive file cover, standard colour is green with yellow stripe. **Classified document register** It is good security practice to keep a record of incoming and outgoing 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. See State Records NSW website for further information on retention and disposal authorities and guidance on information/record retention, disposal, and archiving. If declared by the originator as Accountable Document or Material, it is to have both a reference and copy number. **Disclosure or access** Security clearance to Baseline or above and 'need-to-know'. Only in accordance with legislative and administrative requirements.	**Removal of documents or files** Basis of real need, e.g., meeting. Is to be in personal custody of individual and kept in SCEC-endorsed container e.g., briefcase, pouch, bag. Removal is to be authorised by the manager (or equivalent) responsible for the resource. For home-based work, refer to the *Australian Government physical security management guidelines—Working away from the office* (to be developed). **Audits** It is good security practice to implement spot checks of information at this level.	**Copying** May be prohibited by originator. To be kept to a minimum in keeping with operational requirements. **Physical safe-keeping—minimum standards** Clear desk policy. Agencies are to refer to the *PSPF—Australian Government physical security management guidelines—Security zones and risk mitigation control measures.* **Destruction** ***Paper waste only*** Only appropriate SCEC-approved equipment and ASIO-approved systems are to be used. If Accountable Material, under supervision of two officers cleared to the appropriate level who are to supervise the removal of the material to the point of destruction, ensure that destruction is complete, and sign a destruction certificate. ***ICT media and equipment*** Is to undergo sanitisation or destruction in accordance with ISM.	**Within a single physical location** Single opaque envelope that indicates the classification, receipt at discretion of originator, and either: passed by hand between people who have the appropriate security clearance and 'need-toknow', OR placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger. May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between members of staff with the appropriate clearance and 'need-to-know' and there is no opportunity for any unauthorised person to view the information. **Transfer between establishments within Australia** **EITHER:** Single opaque envelope that does not give any indication of the classification AND placed in an approved briefcase, satchel or pouch and delivered direct, by hand, by an authorised messenger AND receipt required **OR** Double enveloping AND receipt required AND delivered either by SCEC-endorsed overnight courier or by an agency specific alternative approved by ASIO. **Outside Australia** Double enveloping required, receipt required and carriage by DFAT courier service or other authorised officers required.

* Note: this includes information marked **Sensitive: Cabinet** unless it has been marked with a higher classification.

13. Appendix G – Information Classification and Handling Worksheet

Information Asset:	
Classification:	
Information Owner:	
Information Custodian:	
Relevant Governance Requirements e.g. legislative, policy:	
Format: Electronic/Physical/Both:	
Location:	

For each phase of the information lifecycle, identify the parties involved with, or responsible for, information:

Govern	Collect	Organise	Secure	Use	Share	Maintain

Archiving and disposal requirements:	

14. Appendix H – Australian Government Business Impact Levels Guidance

The examples given below are indicative to assist agencies in developing their own business impact level guides.

1 (Low-medium)	2 (High)	3 (Very High)	4 (Extreme)	5 (Catastrophic)
Could be expected to cause **limited damage** to the national interest, organisations or individuals by:	Could be expected to cause **damage** to the national interest, organisations or individuals by:	Could be expected to cause **significant damage** to the national interest, organisations or individuals by:	Could be expected to cause **serious damage** to the national interest, organisations or individuals by:	Could be expected to cause **exceptionally grave damage** to the national interest, by:
Impacts on National Security				
causing limited damage to national security	causing minor damage to national security	causing damage to national security	causing serious damage to national security	causing exceptionally grave damage to national security
Impacts on Agency Operations				
—Operational capacity causing a significant degradation in organisational capability to an extent and duration that, while the agency can perform its primary functions, the effectiveness of the functions is noticeably reduced	causing a severe degradation in, or loss of, organisational capability to an extent and duration that the agency cannot perform one or more of its primary functions	causing a severe degradation in, or loss of, organisational capability to an extent and duration that the agency cannot perform one or more of its functions for an extended time	causing a severe degradation in, or loss of, organisational capability to an extent and duration that the agency cannot perform any of its functions	
—Agency Assets resulting in damage to agency assets	resulting in major harm to agency assets	resulting in major long term harm to agency assets		
—Agency Finances resulting in moderate financial loss to an agency	resulting in substantial financial loss to an agency			
Australian Financial and Economic Impacts				
undermining the financial viability of one or more individuals, minor Australia-based or Australian-owned organisations or companies, or disadvantaging a major Australian organisation or company	undermining the financial viability of, or causing substantial financial damage to, a major Australia-based or Australian-owned organisation or company, or disadvantaging a number of major Australian organisations or companies	undermining the financial viability of, or causing substantial financial damage to, a number of major Australia-based or Australianowned organisations or companies	undermining the financial viability of a number of major Australia-based or Australian-owned organisations or companies in the same sector	
resulting in loss to Australian Government / public sector of $10 to $100 million	resulting in short-term material damage to national finances or economic interests to an estimated total of $100 million to $10 billion	causing long-term damage to the Australian economy to an estimated total of $10 to $20 billion	causing major, long-term damage to the Australian economy to an estimated total in excess of $20 billion	
causing limited damage to international trade or commerce, with the potential to reduce economic growth in Australia	causing material damage to international trade or commerce, with the potential to directly and noticeably reducing economic growth in Australia	causing major, short-term damage to global trade or commerce, leading to short term recession or hyperinflation in Australia	causing major, long-term damage to global trade or commerce, leading to prolonged recession or hyperinflation in Australia	
Impacts on Government Policies				

□ impedes the development of government policies	• seriously impedes the development or operation of major government policies • disadvantaging Australia in international negotiations or strategy	□ significantly disadvantaging Australia in international negotiations or strategy	□ severely disadvantaging Australia in major international negotiations or strategy	
□ resulting in minor loss of confidence in government	□ resulting in a major loss of confidence in government	□ temporarily damaging the internal stability of Australia or friendly countries	□ threatening directly the internal stability of Australia or friendly countries leading to widespread instability	□ resulting in the collapse of internal political stability of Australia or friendly countries

□ causing embarrassment to diplomatic relations	□ causing short term damage or disruption to diplomatic relations	□ causing significant damage or disruption to diplomatic relations including resulting in formal protest or retaliatory action	□ raising international tension, or causing severe damage or disruption, to diplomatic relations	□ directly provoking international conflict or causing exceptionally grave damage to relations with friendly governments
Impacts on Personal Safety				
□ limited harm to individuals – could cause harm to individuals including injuries that are not serious or life threatening	□ endangering individuals - the compromise of information could lead to serious harm or potentially life threatening injury to an individual	□ endangering small groups of individuals - the compromise of information could lead to serious harm or potentially life threatening injuries to a small group of individuals	□ threatening life directly – the compromise of information could reasonably be expected to lead to loss of life of an individual or small group	□ leading directly to widespread loss of life – the compromise of information could reasonably be expected to lead to the death of a large number of people
Impacts on Crime Prevention				
□ hindering the detection, impeding the investigation, or facilitating the commission of low-level crime or hindering the detection of a serious offence, i.e. an offence resulting in 2 or more years imprisonment	□ impeding the investigation of, or facilitating the commission of a serious offence, i.e. an offence resulting in 2 or more years imprisonment	□ causing major, long-term impairment to the ability to investigate serious offences, i.e. offences resulting in 2 or more years imprisonment	□ causing major, long-term impairment to the ability to investigate serious organised crime undertaken by an organised crime group as defined in the *Convention Against Transnational Organised Crime*	
Impacts on Defence Operations				
□ causing limited damage to the non-operational effectiveness or security of Australian or allied forces without causing risk to life	□ causing damage to the non-operational effectiveness or security of Australian or allied forces causing re-supply problems that could result in risk to life	□ causing damage to the operational effectiveness or security of Australian or allied forces that could result in risk to life	□ resulting in severe damage to the operational effectiveness or security of Australian or allied forces	□ causing exceptionally grave damage to the operational effectiveness or security of Australian or allied forces
Impacts on Intelligence Operations				
		□ causing damage to Australian or allied intelligence capability	□ causing severe damage to Australian or allied intelligence capability	□ causing exceptionally grave damage to the effectiveness of extremely valuable security or intelligence operations
Impacts on National Infrastructure				
	□ damaging or disrupting significant State or Territory infrastructure	□ damaging or disrupting significant national infrastructure	□ shutting down or substantially disrupting significant national infrastructure	