Department of Industry

Policy

Classified Information

NUMBER IND-I-196	VERSION 1.1
AUTHORISED BY Chief Information Officer	AUTHORISED DATE June 2016
ISSUED BY Business and Technology Services	EFFECTIVE DATE 01/07/2016

Policy Statement

The NSW Department of Industry, Skills and Regional Development (the "department") is committed to ensuring that all government sensitive information assets are identified and where needed, classified, labelled, handled and appropriately protected to comply with whole of NSW Government requirements. In doing so, the department's information assets will be managed in a manner consistent with the Australian Government security classification system.

Scope

This policy applies to:

- all information held within the department in any format or any location and created on or after 1 July 2015. Information labelled or classified prior to that date does not need to be re-labelled or re-classified unless specifically required due to a business or operational need.
- all personnel who work on behalf of the department, including contractors and consultants (or any other third party who is granted access to the department's information).
- any external parties to which the department has outsourced functions or activities, and therefore associated requirements relating to the management of the department's information assets.

Requirements

1. Whole of NSW Government requirements

a) All staff must comply with requirements defined in the *NSW Government Information Classification, Labelling and Handling Guidelines* that support the implementation of the *NSW Government Digital Information Security Policy* which establishes the digital information security requirements for the NSW public sector.

b) When determining labelling and handling requirements, staff should consider the sensitivity and importance of the record or information, while giving due regard to the impact and consequences of unauthorised use or accidental modification, loss or disclosure and the impact that may have on individuals, organisations, the department, or the government.

2. Handling and Storage of Classified Information

a) Any **classified** information **must not** be created, stored, processed or transmitted within or from the department's information communications and technology (ICT) systems. This applies to classified information created on or after 1 January 2014.

b) If **classified** information is received by email, the sender must be contacted and recipient's obligations to protect the information clearly determined, considering that classified information must not be stored within department's ICT systems.

c) Any **classified** information held within the department must be securely held in a paper based format in accordance with relevant requirements outlined in the Australian Government Protective Security Policy Framework. This must be on a physical file that has been registered in RM8. The current location of the physical file must be maintained in RM8 so that this is up to date at all times.

3. Impact on information access requirements

a) Security protective markings have no effect with respect to legislated requirements for information access, such as the *Government Information (Public Access) Act 2009* (NSW) (GIPAA), the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA), the *Health Records and Information Privacy Act 2002* (NSW) (HRIPA) or 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.

Procedures

- Procedures and advice are available on the department's intranet.

Roles and Responsibilities

The **Office of the CIO** is responsible for:

- administering and updating this policy.
- supporting staff, including consultants, contractors and outsourced service providers as required in order to comply with this policy and its associated procedures or guidelines.

All **Division/Business Unit Managers** are responsible for:

- ensuring that information within their business unit is managed in accordance with this policy and relevant procedures or guidelines.
- ensuring that staff, including consultants, contractors and outsourced service providers, comply with this policy.

All **Staff** are required to comply with the *Classified Information Policy* and any related procedures or guidelines.

Safety Considerations

- None.

Delegations

- None.

Definitions

- **Classified information** is any information displaying the protective security classification markings of **PROTECTED**, **CONFIDENTIAL**, **SECRET** or **TOP SECRET**. The circumstances under when each protective marker should be used are outlined in the *NSW Government Information Classification, Labelling and Handling Guidelines*. By default, any information labelled with the dissemination limiting marker (DLM) of **Sensitive: Cabinet** (Commonwealth) is also considered classified information.
- **Sensitive information** is any information displaying the protective dissemination limiting markings (DLM's) of **Sensitive: NSW Cabinet**, **Sensitive: NSW Government**, **Sensitive: Legal**, **Sensitive: Personal**, **Sensitive: Health Information**, **Sensitive: Law Enforcement**, **Sensitive**, or **For Official Use Only (FOUO)** or that is assessed to warrant the application of that protective marking in accordance with the *NSW Government Information Classification, Labelling and Handling Guideline*s.
- **Unclassified information** is any 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 information is not a security classification or a dissemination limiting marker (DLM).
- **Unmarked information**, or that displaying only a dissemination limiting marker (DLM), is deemed to be UNCLASSIFIED information. This does not apply to information containing only the DLM Sensitive: Cabinet (Commonwealth), as by default that information is automatically deemed to be PROTECTED.
- The term **information assets** within this policy, refers to any form of information and 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, the intellectual information (knowledge) acquired by individuals, datasets, infrastructure, records management systems,

magnetic or optical media, microforms, databases, software applications, hardware and physical assets.

Legislation

- None

Related policies

- NSW Treasury and Finance circular OFS-2015-05-NSW Government Digital Information Security Policy
- *NSW Government Digital Information Security Policy* (V2.0, April 2015)
- *Records Management Policy* (NSW Department of Industry, IND-I-177)

Other related documents

1. **Assessing, labelling and handling information in any format, medium or resource:**
    - *NSW Government Information Classification, Labelling and Handling* Guidelines (V2.2, July 2015)
2. **Assessing, labelling and handling classified information:**
    - *Australian Government Information security classification system* (V2.2, April 2015)
    - Australian Government Protective Security Policy Framework (PSPF)

Superseded documents

- DFS-C2013-05-Information Classification and Labelling Guidelines is replaced by DFSI-2015-01 NSW Government Information Classification, Labelling and Handling Guidelines
- Classified Information Policy TI-A-154
-

Revision history

Version	Date issued	Notes	By
1.0	November 2013	Initial release for approval	Chief Information Officer
1.1	June 2016	Updated to reflect details of review and minor amendments associated with the new versions of related policies and documents	Information Security and Availability Manager

Review date

June 2017

Contact

The Office of the CIO

Email: security@industry.nsw.gov.au