INTERNAL ONLY

ISLHD POLICY COVER SHEET

NAME OF DOCUMENT	Digital Information Data Classification & Labelling Policy
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	ISLHD CORP PD 55
DATE OF PUBLICATION	April 2020
RISK RATING	Low
REVIEW DATE	April 2025
FORMER REFERENCE(S)	N\A
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Chief Information Officer Health ICT
AUTHOR	Business Analyst - Health ICT
KEY TERMS	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance
FUNCTIONAL GROUP OR HUB	Health ICT and Corporate Records
NSQHS STANDARD	Standard One
SUMMARY	This document provides the overarching policy under which information should be handled at Illawarra-Shoalhaven Local Health District

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY

Feedback about this document can be sent to: ISLHD-CorporateGovernance@health.nsw.gov.au

Digital Information Data Classification & Labelling Policy

ISLHD CORP PD 55

1. POLICY STATEMENT

All information is required by the NSW Government to be labelled and classified using a Dissemination Limiting Marker (DLM) which indicates the level of protection required and provides an assurance that it is given an appropriate and consistent level of protection.

Digital data being non-physical, requires a different approach when labelling or classifying it to that of physical data, as the labelling of digital data is an adjunct and not physically on it the classification is applied more a broadly rather than specifically due to the storage and access mechanisms.

The policy defines how digital information can be shared appropriately and securely within ISLHD and with other organisations, individuals, including what levels of permissions need to be obtained prior to disclosing information, what classifications and labelling needs to apply and guides on how the data should be managed.

2. BACKGROUND

This Digital Information Data Classification & Labelling Policy provides ISLHD management and staff guiding principles for the data labelling and classification of digital data during the course of their work.

This policy supports applying information security (InfoSec) across the organisation to ensure data is appropriately classified, managed and protected and is aligned to the NSW Government Information Classification, Labelling and Handling Guidelines DFSI-2015-01 and the NSW Government Managing Data and Information Policy.

Definitions

Health Information

The definition of Health Information according Health Records and Information Privacy Act 2002 No 71.

In the Act, health information means:

a) Personal information that is information or an opinion about:

i. The physical or mental health or a disability (at any time) of an individual;

ii. An individual's express wishes about the future provision of health services to him or her;

iii. A health service provided, or to be provided, to an individual;

b) Other personal information collected to provide, or in providing, a health service;

c) Other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances;

d) Other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of

the health (at any time) of the individual or of any sibling, relative or descendant of the individual.

But does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the Act generally or for the purposes of specified provisions of the Act.

3. RESPONSIBILITIES

This Policy applies to all parties including permanent, temporary and casual staff of Illawarra-Shoalhaven Health, staff seconded from other organisations and contingent workers including labour hire, service providers, professional services contractors and consultants, who may be managing or creating data within the ISLHD digital systems to store data (including systems provided by external providers such as eHealth) with respect to the security and privacy of information.

4. POLICY

This policy covers all digital information owned by or under the control of ISLHD held in a digital format. Non-digital data is not covered by this policy.

Once data is identified as requiring protection and special handling, a protective marking called a Dissemination Limiting Marker (DLM) is to be assigned to the information. The marking indicates:

- The level of confidentiality the information needs; and
- The level of protective procedures that are to be provided during the use, storage, transmission, transfer and disposal of the information.

All information must be have a DLM applied accordingly as indicated below;

- For Office Use Only (FOUO) also known as Sensitive.
- Sensitive: Health or patient data
- Sensitive: Personal or private data
- Sensitive: Legal
- Sensitive: Commercial
- Public
- Sensitive: NSW Government
- Sensitive: NSW Government Cabinet

The default information classification is For Office Use Only (FOUO) and should be marked so where possible in order that people know how to handle it appropriately.

This means that access to this information is restricted to ISLHD staff with a ‘need to know’ and third parties under a non-disclosure or confidentiality agreement with ISLHD.

Therefore any information without a classification label is considered classified as "FOUO".

4.1 PRINCIPLES

In NSW, two additional DLMs are used when communications are destined for the NSW Government, which are;

a) Sensitive: NSW Government

b) Sensitive: NSW Cabinet

The default Information classified as For Office Use Only (FOUO) should be marked so where possible in order that people know how to handle it appropriately.

This means that access to this information is restricted to ISLHD staff with a 'need to know' and third parties under a non-disclosure or confidentiality agreement with ISLHD.

Therefore any information without a classification label is considered classified as "FOUO".

4.1.1 Information Classification

ISLHD is to use the following classification levels for confidentiality of information in line with the Australian Government Security Classification System which uses Dissemination Limiting Marker (DLM).

A DLM: Dissemination Limiting Marker is a type of security classification to grade the confidentiality requirements of official information, prescribed under the Australian Government Information Security Management (ISM) guidelines. DLM marking is used for information where disclosure may be limited or prohibited by legislation, or where special handling of the information is required.

Dissemination Limiting Markers [DLMs]	**Description**
For Official Use Only (FOUO). Also known as Sensitive.	FOUO is applied to unclassified information that is only available **f**or **o**fficial **u**se **o**nly by ISLHD when its compromise may cause limited damage to ISLHD organisation or individuals. The public release of this information may be authorised by Customer Service and Corporate Governance.
Sensitive: Personal & Health (SP)	Personal & Health classification is to be used when the information contains personal attributes which may include such things as an individual's fingerprints, retina prints, body samples, genetic characteristics, political beliefs, or sexual preferences. A compromise could;

	i. Endanger individuals and private entities – the compromise of information could lead to serious harm or potentially life threatening injury to an individual ii. Work substantially against state or national finances or economic and commercial interests. iii. Substantially undermine the financial viability of ISLHD. iv. Impede the investigation or facilitate the commission of serious crime, or v. Seriously impede the development or operation of major government policies. This aligns with the definition of sensitive information in Section 6 of the Health Records and Information Privacy Act 2002 (NSW), Ref: **Error! eference source not found. Error! Reference source not found.**.
Sensitive: Legal (SL)	Legal classification is be used for any information that may be subject to legal professional privilege. A compromise could cause limited damage to ISLHD corporate or staff, an agency, commercial entities or members of the public.
Sensitive: Commercial, (SC) or NSW Government	The Commercial/Cabinet classification is to be used where compromise could: a) Endanger individuals and/or private entities b) Work substantially against ISLHD or NSW State, finances, economic and commercial interests. c) Substantially undermine the financial viability of ISLHD. d) Impede the investigation or facilitate the commission of serious crime. e) Seriously impede the development or operation of ISLHD or NSW Govt policies. May be used for any information that may be subject to commercial in confidence. Information that was previously labelled as Protected under the NSW labelling system may translate to the DLM Sensitive: NSW Govt.
Sensitive: Cabinet (SC).	Sensitive: Cabinet is to be applied to: a) 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, or b) official records of Cabinet c) any other information that would reveal: — The deliberations or decisions of Cabinet, or — 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 or Secret. A summary guide on identifying information requiring a marking is at Annex A: Classification and marking ready-reckoner chart.
Public	Information authorised for unlimited public access and circulation, such as agency publications and web sites. Such information should still be accompanied by Integrity and Availability classifications and may need to be approved for classification as public by the relevant department such as Customer Service and Corporate Governance.

The following sub-topics further expand on the definitions in order to facilitate a better understanding of data classification and reduce ambiguity.

4.1.2 Information classified as *FOUO or General-Business* includes:

a) Routine correspondence
b) Employee newsletters
c) Internal phone directories
d) Inter-office memoranda
e) Non person-identifiable information
f) Internal policies and procedures

Consequences if information is mishandled:

g) Unauthorised disclosure would not significantly impact ISLHD, or any stakeholders or employees

For Office Use Only (FOUO) classification, this is sometime seen titled as sensitive when referred to in Australian Government documents.

4.1.3 Information classified as Personal (Health) includes:

a) Person-identifiable information (including employee information except that which is classified more restricted under Legal).
b) Information that is person identifiable and which has been provided by a patient or collected by the LHD or any other care provider for the purpose of supporting the care of that patient (except that which *more restricted*).

Consequences if information is mishandled:

c) Unauthorised disclosure could result in significant adverse impact or penalties to ISLHD corporate and staff or other stakeholders.

d) Unauthorised disclosure could result in significant adverse impact on a patient, or penalties to ISLHD.

4.1.4 Information classified as Legal includes:

a) Statutorily protected and sensitive information as defined in the *NSW Government and Labelling Guidelines*.

Consequences if information is mishandled:

b) Unauthorised disclosure likely to result in significant adverse impact, embarrassment or penalties to NSW Health, its stakeholders or employees

4.1.5 Information classified as *Commercial or Cabinet* includes:

a) Financial data.

b) Purchasing information.

c) Official records that are submitted or proposed to be submitted to Cabinet.

d) Any other information that would reveal Cabinet deliberations.

e) Vendor contracts.

f) Closed-circuit television (CCTV) recordings.

Consequences if information is mishandled:

g) Unauthorised disclosure could result in significant adverse impact or penalties to ISLHD, patients, other stakeholders or employees

4.1.6 Information classified as *Public* includes:

a) Brochures

b) News releases

c) Marketing Materials

Consequences if information is mishandled:

d) None

4.1.7 Data Custodians or Information Asset Stewards

A register of Data Custodians (or Information Asset Stewards) should be maintained by the Senior Information Risk Officer. They will generally be the individuals who are employed by the LHD or contracted to the LHD to manage information resources and may include:

a) Managers of medical records departments
b) Managers of corporate records departments
c) Managers of departments who source IT services from non-NSW Health service providers
d) Managers of service departments with their own IT functions
e) Managers of departments who maintain their own patient record repositories
f) The Chief Information Officer

Principles of Classification

Classification Review

Data classification should be review annually by conducting a risk assessment by the data custodians and business/ department managers.

For example; Information may require a lower classification over time, e.g.: an annual report in its compilation stage may be classed as “FOUO”, however, once published it is likely to become “Public”.

Data Aggregation Classification

Information records such as archives will contain various records and are therefore likely to contain information with varying classifications. The following are examples of aggregated media which must fall back to the highest classification of the data that is contained within;

a) Archive data
b) Data hosts, drives, media, IT systems
c) Communications links.

Data repositories and communications are to be managed according to the requirements of the highest classification of data held or transmitted.

External & Third Party Information

Ensure that the information classification is understood and applied as expected.

Internal Information Handling

Information may be disclosed between ISLHD departments without additional control above and beyond those required by legislation and other relevant policy documents.

Refer to Appendix A for specific guidelines on how information is to be handled according to its classification.

Compliance and Enforcement

Failure to comply with any element of this policy may result in disciplinary action advised by HR in accordance with ISLHD Employee Disciplinary Policy and Procedures.

4.2. PROTECTIVE MARKINGS

4.2.1 When to security classify information

There are four levels of security classification. These classifications reflect the level of damage done to the national interest, organisations and individuals of unauthorised disclosure, or compromise of the confidentiality, of information:

a) Protected
b) Confidential
c) Secret
d) Top secret.

Departments must determine in which circumstances security classifications are to be applied to its information.

4.2.2 Protected

The Protected security classification should be used when the compromise of the confidentiality of information could be expected to cause damage to the national interest, organisations or individuals.

For instance, where compromise could:

a) Endanger individuals and private entities – the compromise of information could lead to serious harm or potentially life threatening injury to an individual
b) Work substantially against NSW Government or ISLHD finances or economic and commercial interests
c) Substantially undermine the financial viability of ISLHD.
d) Impede the investigation or facilitate the commission of serious crime, or
e) Seriously impede the development or operation of ISLHD and major government policies.

4.2.3 Confidential

The Confidential security classification should be used when the compromise of the confidentiality of information could be expected to cause significant damage to the national interest, NSW Government Cabinet, ISLHD and its affiliates or individuals.

Confidential may be applicable to ISLHD.

For instance, where compromise could:

a) Endanger small groups of individuals – the compromise of information could lead to serious harm or potentially life threatening injuries to a small group of individuals

b) Damage relations – in other words, cause formal protest or other sanction

c) Damage operational effectiveness or security of Australian or allied forces

d) Damage the effectiveness of valuable security or intelligence operations disrupt significant national infrastructure, or

4.2.4 Secret

The SECRET security classification should be used when compromise of the confidentiality of information could be expected to cause serious damage to the national interest, organisations or individuals. Secret classification is not applicable to ISLHD.

4.2.5 Top Secret

The TOP SECRET security classification requires the highest degree of protection as compromise of the confidentiality of information could be expected to cause exceptionally grave damage to the national interest. Top Secret classification is not applicable to ISLHD.

4.2.6 Applying Caveats

The Australian and the NSW Government outline the use of caveats where the caveat is in addition to the current data classification increasing the security level in particular relating to Australian Government security operations.

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

NSW agencies including ISLHD that handle information requiring security classification must manage this information in accordance with Commonwealth requirements. Only a small number of agencies deal with information at this level.

Security classifications Confidential, Secret and Top Secret are to be regarded as national security classifications under these Guidelines.

4.3 EXEMPTIONS

Any exemptions to this policy must be approved by the Chief Information Officer (CIO) or Health ICT Deputy Director after a risk assessment has been completed. Written approval for exemption must be completed through a Brief and must be recorded within the Document Management System (i.e. TRIM) as per the ISLHD Records Management Standard.

4.4 DATA MAINTENANCE AND PRESERVATION.

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 and preservation can mean many things, for instance it could involve:

a) Information de-classification over time

b) Ensuring sensitive information can still be decrypted

c) 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.

5. DOCUMENTATION

The following documents may assist in providing guidance in applying DLMs to digital data.

- HICT Directory Permission Assignment Standard T19/2285

6. AUDIT

Annually

7. REFERENCES

The following documents are referenced in this policy:

Legislation, Policies and Guidelines.

a) ISLHD Information Security Policy PD 38

b) NSW Government Cyber Security Policy.

c) Electronic Information Security Policy – NSW Health

d) NSW Government Classification Labelling and Handling Guidelines.

e) Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act).

f) Health Records and Information Privacy Act 2002 (NSW) (HRIP Act).

g) Australian Government Security Classification system

Standards

a) ISO 27001:2013 Information technology - Security techniques - Information security management systems.

b) ISO/IEC 27002:2013. Information Technology - Security Techniques - Code of Practice for Information Security Management.

c) ISO 31000 Risk management - Principles and guidelines

8. REVISION & APPROVAL HISTORY

Date	Revision No.	Author and Approval
May 2019	0	Program Manager ICT Security & Strategy. **Approval/Date:** Director Corporate Services/Chief Information Officer
April 2020	1	Business Analyst – Health ICT **Approval/Date:** Corporate Policy Recommendation committee / April 2020 **Approval/Date:** Chief Information Officer / April 2020

9. APPENDIX 1 - Handling Guidelines for Dissemination Limiting Markers (DLM)

Creation and Storage

FOUO	Sensitive: Personal	Sensitive: Commercial	Sensitive: Legal (SL)	Sensitive: Health Information (SH)	Sensitive: Law Enforcement (SE)
The controls applied for the storage of any information marked FOUO 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,	FOUO (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.	FOUO (Minimum Controls) must be applied.	FOUO (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	FOUO (Minimum Controls) and Sensitive: Personal controls plus: Sensitive health information should be collected in accordance with the Health Records and Information Privacy Act 2002 and the Privacy and Personal Information Protection Act 1998 Both can be found at; http://www.islhd.health.nsw.gov.au/Privacy.asp 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.	FOUO (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

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			Privilege are required to be marked with Sensitive: Legal. Non-disclosure of Sensitive: Legal documents must be strictly observed to preserve Client Privilege.	Refer to Statutory Guidelines and Health Privacy Principles published on Information and Privacy Commission web site. (http://www.ipc.nsw.gov.au/hriphttp://www.ipc.nsw.gov.au/hrip-actact) ISLHD 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	legislative requirements as well as the corresponding requirements stated in the Guidelines.

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.				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) and http://www.islhd.health.nsw.gov.au/Privacy.asp	

Information Classification, Labelling and Handling Guidelines

Dissemination and use

FOUO (Sensitive)	Sensitive: Personal	Sensitive: Commercial	Sensitive: Legal	Sensitive: Health Information	Sensitive: Law Enforcement
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	FOUO (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,	FOUO (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	FOUO (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.	FOUO (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.	FOUO (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

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	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.	the Office provides further assistance.	For example: Legal advice must be kept confidential throughout the agency in order to preserve the client's rights to claim Client Privilege.	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) and http://www.islhd.health.nsw.gov.au/Privacy.asp	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

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.					the information warrants this level of protection.

Information Classification, Labelling and Handling Guidelines

Archiving and Disposal

FOUO (Minimum Controls) (Sensitive)	Sensitive: Personal	Sensitive: Commercial	Sensitive: Legal	Sensitive: Health Information	Sensitive: Law Enforcement
Information labelled FOUO 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. Departments 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	FOUO (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.	FOUO (Minimum Controls) must be applied.	FOUO (Minimum Controls) must be applied.	FOUO (Minimum Controls) plus: General guidance could also be sought from AS/ISO27799 Information security management in health using ISO/IEC 27002	FOUO (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.

Records' website for further information on retention and disposal authorities and guidance on information/record retention, disposal, and archiving. FOUO 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. FOUO 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.					