Australian Government
Fair Work Building & Construction

Australian Government
Fair Work OMBUDSMAN

Agency Security Information Classification & Handling Guidelines
July 2012

CHANGE HISTORY

Update the following table as necessary when this document is changed:

Name	Date	Nature of Change
Craig Smith	3/05/2012	Draft development
Craig Smith	7/06/2012	2nd Draft
Chris Cahill	20/6/2012	DLM Matrix amended to include Operations In Confidence
Chris Cahill	31/7/12	Final amendments to draft

Table of Contents

1. Overview

Except where otherwise specified, these guidelines apply equally to the Fair Work Ombudsman (FWO) and Fair Work Building and Construction (FWBC), known from this point forward as the 'Agency'.

2. Policy Framework

2.1 Security Policy and Guidelines

The Protective Security Policy Framework (PSPF) and Australian Government Information Security Manual (ISM) set out the policies, practices and procedures with which all Australian Government Departments and Agencies must comply.

Security policy and guidelines highlight the Agency's commitment to preserving the confidentiality, integrity and availability of all information provided to the Agency, or generated from within. This commitment takes into account a number of factors, including the following:

- our reputation as a responsible custodian of sensitive client information is a significant factor contributing to community confidence in our operations;
- legislation administered by the Agency's imposes certain obligations in relation to information security;
- the imperatives of meeting our business outcomes;
- legislation, such as the *Crimes Act 1914* and *Privacy Act 1988*, requires us to safeguard information. The full text of the ***Crimes Act 1914, Criminal Code 1995, Freedom of Information Act 1982*** and ***Privacy Act 1988*** can be viewed at www.comlaw.gov.au. and;
- relevant Australian Government policies, associated guidelines and framework.

2.2 Access to Information

To reduce the likelihood of information being lost, destroyed, damaged, compromised or misused, access to the Agency's information is only authorised if all the following conditions are met:

- there is a genuine 'need to know'
- access will comply with legislative requirements;
- there is no conflict of interest regarding the information; and
- the person has the required level of security clearance.

2.3 Need to Know

A person has a genuine 'Need to Know' if, without access, they would be hindered in the performance of their duties. Employees are not entitled to access information merely because it would be convenient for them to know, or by virtue of status, rank or level of security clearance.

Agency employees should ensure that disclosure of official informationis in accordance with Government guidelines and instructions. Employees who have questions or concerns about the disclosure of official information should take up the matter with their supervisors and/or managers.

2.4 Clear Desk Policy

Employees must ensure information requiring a Dissemination Limiting Marker (DLM) or a classification and other valuable resources are secure when absent from their work point, if the absence would allow unauthorised access to information or resources.

The clear desk policy also means that employees must ensure electronic information is protected from unauthorised access. During short absences, the smartcard should be removed from the reader, and during longer absences the computer should be logged off.

At the close of business each day employees must take precautions to ensure information is safeguarded from unauthorised access. This includes:

- shutting down all systems and networks;
- securing all information requiring a DLM or a classification;
- ensuring all security containers and safes are locked; and
- making sure all keys to security containers are secure.

2.5 Outside the office

Employees undertaking field based work, work related travel or home based work need to ensure the Agency's information is safeguarded against unauthorised access. This includes:

- packaging and carrying information appropriately;
- protecting information from unauthorised viewing in public places;
- ensuring security of hard copy information and IT equipment; and
- controlling access to information in the home environment.

3. Security Classifications and Markings

3.1 Two types of official information

Information includes data from any source and in any form (including voice and electronic), which is collected, received, stored or developed by the Agency or its employees, and includes intellectual knowledge.

The PSPF places all official information handled by government agencies under two main categories:

- Information that does not need increased security; and
- Information that needs increased security to protect its confidentiality.

Official information can include public sector information sanctioned for public access or circulation, such as agency publications or web sites.

Official information not needing protection may be marked UNCLASSIFIED.

3.2 Who is responsible for the decision to apply protective markings?

The person responsible for preparing the information, or for actioning, is to decide its protective markings. This person is called the **originator** (i.e. the author).

3.3 Who can alter a protective marking?

Only the originating agency, in other words, the agency that assigned the original protective marking can change the markings it applies to its information. If an agency is abolished or merged, the agency assuming the former agency's responsibilities is considered the originating agency.

Protectively marked records transferred into the custody of the National Archives of Australia keep the protective markings they had when received from the originating agency and are stored and handled in accordance with those markings.

3.4 When to apply protective markings

When information is created, the originator is required to assess the consequences of damage from unauthorised compromise or misuse of the information. If adverse consequences could occur or the agency is required to protect the information it is to be given a protective marking.

Classifying includes documents, files, removable hard disk drives, laptops, Ipads, video and audio tapes, USBs or any form of information. Any portable media used to store classified information must be marked appropriately, and destroyed in line with the requirement set out within the Information Security Manual (ISM).

3.5 Over classification

Information should only be classified when the consequences of the compromise warrants the expense of increased security protection. It is important that information not requiring protection remains unclassified.

Inappropriate over-classification has many seriously harmful effects such as:

- the general public's access to government information becomes unnecessarily limited;
- unnecessary or costly administrative arrangements are established, which remain in force for the life of the document (including repository arrangements for records transferred to National Archives of Australia);
- the volume of security classified information becomes too large for an agency to adequately protect; and
- classification and security procedures are brought into disrepute if the classification is unwarranted (this may lead to classifications and protective markings in general being devalued or ignored by employees or receiving agencies).

For these reasons the government expects that the Agency will only classify information and maintain that classification when there is a clear and justifiable need to do so.

3.6 Limiting the duration of a security classification

When first classifying information the originator should try to settle a specific date or event for declassification based on an assessment of the duration of the information's sensitivity. On reaching the date or event the information should be automatically declassified.

If the originator cannot decide an earlier specific date or event for declassification, information should be marked for declassification 10 years from the date of the original decision.

An originator may extend the duration of security classification, change the security classification, or reclassify specific information only when the protocols and guidelines for security classifying information are followed.

Cabinet documents are not included in such arrangements.

3.7 How to identify information to be security classified

Official information that requires increased protection and does not meet the definition of security classified information is most often about:

- government or agency business, where compromise could affect government capacity to make decisions or operate, public confidence in government and stability of the market place;
- commercial interests, where compromise could affect the competitive process and provide the opportunity for unfair advantage;
- personal information that is required to be protected under provisions of the *Archives Act 1983*, *Privacy Act 1988*, or other legislation.

Not all information about these matters needs to be security classified. Information is only to be security classified if the compromise could cause damage.

A summary guide on identifying information requiring a security classification is at **Annex A: Classification and marking ready-reckoner chart**.

4. Protective Markings

4.1 Three types of Protective Markings:

Once information has been identified as requiring some form of protection and special handling a protective marking is to be assigned to the information. The marking indicates:

- that the information has been identified as sensitive or security classified, and
- the level of protective procedures that are to be provided during the use, storage, transmission, transfer and disposal of the information.

A protective marking indicates the required level of protection to all users of the information. The system, therefore, provides an assurance that information of broadly equivalent worth or value is given an appropriate and consistent level of protection.

Information requiring a protective marking that is held on ICT systems is to be identified in the same way as information held on other mediums, such as, paper documents and given an appropriate level of protection.

There are three types of protective markings:

- security classifications
- dissemination limiting markers (DLMs), and
- caveats.

4.2 Security classifications

Security classification information is information relating to Australia's security, defence, international relations, or national interest. There are four security classifications which reflect the consequences of unauthorised disclosure of information:

- PROTECTED;
- CONFIDENTIAL;
- SECRET; and
- TOP SECRET.

It is not envisaged that the Agency would be required to create or handle this level of information.

For information on the handling and control procedures for security classified information, consult the Agency Security Advisor.

4.3 Dissemination limiting markers

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

The agency is responsible for determining the appropriate protections to be applied to information bearing DLMs, except Sensitive: Cabinet, by ensuring that the following principles of good information security practice are applied:

- information can 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 the Agency's premises is on the basis of identified need;
- disposal of information is by secure means; and
- transmission and transfer of information is to be by means which deter unauthorised access: for example, external mail is sealed and electronic transmission is in accordance with ISM requirements.

The following five categories of DLM are used:

4.3.1 For Official Use Only (FOUO)

- **For Official Use Only (FOUO)** may be used on unclassified information only, when its compromise may cause limited damage to national security, Australian Government agencies, commercial entities or members of the public.

4.3.2 Sensitive

- **Sensitive** may be used with security classified or unclassified information:

  a) where there is a requirement for secrecy under legislation;
  b) the disclosure of which may be limited or prohibited under legislation; or
  c) which may fall under the category of an 'exempt document' under the FOI Act Part IV Section 38.

  The Agency is required to apply the Sensitive DLM in the header and footer as well as identify the reason the DLM has been applied and any special handling requirements either in the footer or as a cover page. For example:

  > *This information is "protected information" as described in Section 56 of the Australian Prudential Regulation Authority Act 1998 and may only be accessed by APRA officers.*

4.3.3 Sensitive: Personal

- **Sensitive: Personal** is applied to any unclassified or classified information:

  a) that may fall under the category of documents affecting personal privacy under the FOI Act Part IV Section 47F 'Public interest conditional exemptions-personal privacy', and
  b) is 'sensitive information' as interpreted under the *Privacy Act 1988* Part II Section 6.

  Such information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. It can include:

a) Information or an opinion about an individual's:
   i. racial or ethnic origin
   ii. political opinions
   iii. membership of a political association
   iv. religious beliefs or affiliations
   v. philosophical beliefs
   vi. membership of a professional or trade association
   vii. membership of a trade union
   viii. sexual preferences or practices, or
   ix. criminal record
b) health information about an individual; or
c) genetic information about an individual that is not otherwise health information.

4.3.4 Sensitive: Legal

- **Sensitive: Legal** is to be applied to any unclassified or classified information which may fall into the category of 'documents subject to legal professional privilege' under the FOI Act Part IV section 42**:**

a) a document is an exempt document if it is of such a nature that it would be privileged from production in legal proceedings on the ground of legal professional privilege;
b) a document is not an exempt document because of subsection (a) if the person entitled to claim legal professional privilege in relation to the production of the document in legal proceedings waives that claim;
c) a document is not an exempt document under subsection (a) by reason only that:
   i. the document contains information that would (apart from this subsection) cause the document to be exempt under subsection (a); and
   ii. the information is operational information of the Agency.

The person marking the information needs to be assured that the information is subject to legal privilege.

4.3.5 Sensitive: Cabinet

- It is to be applied to any information which may fall under the category of 'Cabinet documents' as defined in the FOI Act Part IV Section 34.

Cabinet documents and matters considered by Cabinet or decisions of Cabinet (or a Cabinet committee) include:

a) business lists for meetings of the Cabinet and its committees;
b) Cabinet programmes and notices of meetings;
c) Cabinet submissions and memoranda, including copies lodged with the Cabinet Secretariat and copies held elsewhere;
d) corrigenda to submissions and memoranda;
e) reports and attachments to submissions and memoranda (whether or not actually attached) which have been brought into existence for the purpose of being considered by the Cabinet;
f) schedules circulated for ministers' information, for example, schedules of appointments, endorsements or matters without submission;
g) any papers circulated by ministers in the Cabinet room related to matters under discussion by the Cabinet;
h) any papers circulated by the Cabinet Secretariat on behalf of the ministers for consideration by the Cabinet as matters without submission or slides used by ministers in presentations to Cabinet;

i) correspondence between ministers and the Prime Minister which is submitted to the Cabinet or proposes matters (including appointments) to be raised in Cabinet without submission;
j) Cabinet and Cabinet committee minutes;
k) documents of the Cabinet Secretariat including Cabinet notebooks or other material that in any way records the deliberations of Cabinet; and
l) copies of, or extracts from, documents referred to above.

The Sensitive: Cabinet DLM can only be applied to classified information which must be marked PROTECTED at a minimum, for example: PROTECTED Sensitive: Cabinet. This is to remove any confusion about the minimum level of control and security clearance needed to access Cabinet material.

A summary guide on identifying information requiring a marking is at **Attachment A:** Classification and marking ready reckoner chart.

The Agency will choose whether to use DLM's, other than Sensitive: Cabinet, on a case-by-case basis. The presence or absence of such a marking will not affect a document's status under FOI Act.

4.4 Caveats

Caveats only relate to National Security classified Information and will not be required for the Agency. Further information can be sourced from the Agency Security Advisor.

5 Procedures for applying Protective Markings

5.1 Marking of DLMs and security classifications

Security classifications and caveats are to be in capitals, bold text and a minimum of 5 mm high (preferably red) - for example, **PROTECTED** or **CONFIDENTIAL**. DLMs are marked using capitals for each word, in bold text and a minimum of 5 mm high (preferably red) – for example, **For Official Use Only** or **Sensitive**. Further examples of the positioning of a protective marking are displayed at **Attachment B**. For further clarification of marking security classified information, contact the Agency Security Advisor.

Classification markings must be conspicuously marked at the top and bottom of each page at the time a document is first created. Bound books and pamphlets must also show the classification on the front cover, title page, rear cover and, where possible, on the spine of the document.

When a DLM of 'Sensitive' is used, it must include a footer on the first page, or a separate cover page, that identifies the reason for the 'Sensitive' marking and the handling requirements for the document as a result of the marking.

Example: Front page

Sensitive

.....

<Reason for marking, e.g. This document may contain 'Sensitive information' as defined under the *Fair Work Act 2009*>

Sensitive

Cover sheet

The attached document contains Sensitive information

<Reason for marking, e.g. This document may contain 'Sensitive information' as defined under *the Fair Work Act 2009*

This document is to be handled.....>

5.2 Protective marking Cabinet documents

All documents prepared for consideration by Cabinet, including those in preparation are, as a minimum, to be protectively marked 'Sensitive: Cabinet' and carry the security classification PROTECTED, regardless of any other security consideration. For an example see **Attachment B**.

5.3 Emails

The protective marking of an email must be equal to the highest classification applicable to the email subject line, the contents of the email and the classification of any documents attached to the email.

5.4 Files

The protective marking of a file must be equal to the highest marking of any item of information within the file. The reverse, however, does not mean information being placed within a file automatically takes on the same protective marking as the file. Each item of information needs to be protectively marked in its own right.

Certain compilations of information may require a higher protective marking than that of their specific parts because the combination of the information creates a greater value and an increased likelihood of compromise. Additionally, the unauthorised access to and disclosure of the whole file could potentially result in greater damage than compromise of a component. This is normally referred to as 'aggregation', and particularly relevant to large collections of electronic information.

Sometimes a single item of information can cause a whole file to attract a higher protective marking. This may unnecessarily restrict access to the majority of the information on the file. In this case, it may be desirable and convenient to open another file with a higher protective marking to hold this single item, and then make reference to this on the original file.

5.5 Reproduction of protectively marked documents

Protectively marked information should be reproduced only when necessary. Spare or spoilt copies should be destroyed immediately and in accordance with the procedures for destruction of protectively marked documents and ICT media. This destruction is defined as 'normal administrative

practice' in terms of the Archives Act and does not need specific permission from the National Archives of Australia.

To make copies of protectively marked information that has a copy number, the originating agency's permission is required. It is preferable that any additional copies be provided by the originator.

Should the originator give permission for the receiving agency to copy the information, agencies should provide the proposed additional distribution to the originator. The originator will indicate the appropriate additional copy numbers which are to be clearly marked on the additional copies.

5.6 Discussing sensitive information

Positive action must be taken by employees to ensure conversations of a sensitive nature are not overheard by unauthorised persons.

Sensitive information must not be discussed in public places such as coffee shops, lifts, airport lounges, restaurants, bars, on public transport, or at social functions (especially when using phones).

Where PROTECTED or Sensitive: Cabinet information is to be discussed at meetings, all persons present must have a genuine 'need to know' and appropriate security clearance. Any notes or minutes from the meeting will need to be classified in their own right.

5.7 Previously classified information

The protective markings of information received from another government agency cannot be changed without the approval of that agency. Agencies must be consulted when protective markings are thought to be unsuitable.

Any sensitive or security classified material received from other agencies must be afforded the minimum security protection standards required for the material.

5.8 Non-government protective markings

At times the Agency will receive information from non-government sources bearing labels similar to our protective markings. For example, the material might be marked CONFIDENTIAL or COMMERCIAL-IN-CONFIDENCE.

Generally speaking, there is an expectation on the part of the client that the information will be appropriately safeguarded. Whilst the Agency should attempt to provide an adequate level of protection to the material as intended by the document originator, the Agency should independently assess the sensitivity of the material to determine whether it warrants an Australian Government protective marking.

5.9 Electronic storage media and equipment

Removable media such a hard disk drives, USB Drives, and CD's are to be marked to indicate the protective marking of the stored data. The media must be safeguarded in the manner prescribed for the highest protective marking recorded thereon until the material is reclassified or the media is destroyed. Password protection with encryption is strongly recommended where the removable media is regularly taken outside agency premises.

Where possible, the protective marking of information retrieved from such media must be displayed on the screen, or on any hard copy produced.

5.10 Review and reconciliations

Managers must ensure reviews of Sensitive information are conducted at regular intervals within their area of control.

The purpose of these checks is to verify material is accounted for, protective markings are still valid and that handling and storage procedures meet the standards set out in this guideline.

5.11 Reclassifying information

When sensitive or security classified information changes it must be reclassified as soon as possible. The reclassification process refers to both the downgrading and upgrading of security classifications. Where reclassification is considered warranted the standards and guidelines for the classification of information must be reapplied.

The approval to downgrade sensitive or security classified information must be from the originator. Managers may issue procedures for downgrading sensitive or security classified information originating in their area of control, but material classified by another area or agency requires the permission of the originating area or agency.

When a reclassification is carried out, all recorded holders of the information in question are to be advised, and the marking of the classification on all copies amended.

5.12 Recording of reclassification

On documents, cross out the superseded marking and insert the new marking alongside, together with the initials of the person making the entry and the approval to upgrade or downgrade the material.

Where it is necessary to change the classification of a file, the superseded file cover should be retained inside the new file to preserve the previous history of the records. Files are to be reclassified only in response to changes to the classification of their contents.

For electronic media, a record should be maintained of previous classifications and dates of classification change.

6 Storage requirements

6.1 Security Storage Containers

The PSPF specifies minimum storage standards for the protection of official information.

The following details the storage requirements for information within the Agency's premises:

- **PROTECTED & Sensitive: Cabinet**
  - SCEC endorsed 'C' Class container (Bi-Lock controlled cabinet)
- **DLMs (FOUO, Sensitive, Sensitive: Legal and Sensitive: Personal)**
  - lockable commercial grade container (e.g. Compactus/steel lockable grade container)
- **Unofficial – Public Release**
  - no restrictions

Where security storage requirements cannot be met, contact the Agency Security Advisor.

6.2 Electronic storage

Information stored electronically is subject to the same level of protective security as paper-based information.

Consideration must be given to the 'Need-to-Know' principle and ease with which unauthorised people could gain access.

The security of the Agency's network is not currently of a standard sufficient to protect information classified above Sensitive.

7 Removal or transfer of protectively marked documents and materials from the Agency's premises

7.1 Movement of classified information

The movement of information increases risk. The principles for secure movement of information involve:

- timely and uninterrupted handling;
- secure methods of packaging, transport and delivery;
- supervision and recording of all handling processes; and
- the allocation of specific responsibilities to those involved with the movement of information.

The following information outlines the movement and packaging requirements for:

- Unofficial
- FOUO
- Sensitive (including Sensitive: Legal or Personal)
- PROTECTED (including Sensitive: Cabinet)

7.2 Opening requirements

Employees should look for any signs of tampering when opening envelopes or wrapping on classified material.

When it is known or suspected that an envelope or package containing classified material has been tampered with, the matter must be reported to the manager of the area and the Agency Security Advisor.

The envelope or package is to be retained for examination and not opened or handled unnecessarily.

7.3 Security wafer seals

Security wafer seals are designed to show evidence of tampering during transit and their use varies according to the security classification of the material.

Supplies of security wafer seals can be obtained from the Agency Security Advisor. Security wafer seals must be locked in a 'C' Class security container when not in use.

7.4 Bulk packaging

One of the main principles of security packaging is to prevent the theft, interference, or damage to classified material and to provide evidence of tampering.

Where the volume of information or type of media makes it impracticable to use envelopes, alternatives include the use of boxes with appropriate layers of wrappings , or appropriate security containers.

Particular care should be taken with large quantities of classified material. Advice regarding the bulk transmission of classified material is available from the Records Management area.

7.5 Electronic transfer

Specific measures are required to protect security classified information moved electronically.

The following information outlines how to electronically transfer information for:

- Unofficial
- FOUO
- Sensitive (including Sensitive: Legal of Personal)
- PROTECTED (including Sensitive: Cabinet)

7.6 Verbal briefings

When it is necessary to provide information classified as FOUO, Sensitive or PROTECTED to a number of people, the use of verbal briefings (in the appropriate environment) could be used as an alternative to circulating sensitive documents.

Action must be taken by people delivering verbal briefings to ensure all persons present have a genuine need to know and the appropriate level of security clearance. Agency personnel seeking confirmation of another staff-member's clearance should contact the Agency Security Advisor prior to the briefing commencing.

7.7 Safe hand

'Safe Hand' is the term used to describe the process of dispatching material to an addressee in the care of an authorised person, or succession of authorised persons, responsible for its carriage and safekeeping.

At each hand-over a receipt is obtained identifying the package, time and date of the hand-over, as well as the name and signature of the recipient. At no time is the article out of the direct control of one of the authorised employees, or by couriers approved for the transmission of security classified material. A list of approved couriers can be obtained from the Agency Security Advisor.

7.8 Removal of classified material from the office

The removal of information protectively marked FOUO or Sensitive from the office is only permitted where there is a definite work related need, appropriate protection can be maintained, and the removal is authorised by the manager responsible for the information.

It is imperative to be able to trace/record the movement of the information (i.e. notation in trim). Should you require further assistance contact the Records Management Team.

Digital media stored on devices such as smart phones, laptops, Ipads, disks and USB drives which carry information that is protectively marked FOUO or Sensitive, must be safeguarded with password protection.

All portable electronic devices carry additional risk when storing FOUO or Sensitive information as their value makes them a target.

Data transferred or stored onto Cloud based services (e.g. Skydrive, Gdrive, Dropbox) including hosted email services (gmail, hotmail) will pose additional security risks including sovereign as the data will be stored on equipment in foreign countries with differing legal jurisdictions in regards to disclosure of information. Particular care must be taken in storing or transferring FOUO and Sensitive information with such services and should only be authorised by the manager responsible for the information.

Employees removing classified material from the office have an important role in the protection of that material. As such, employees must take practical measures to ensure security classified material is safeguarded at all times and safeguarded against unauthorised access.

A number of secure briefcases have been endorsed for the carriage of security classified information. The Agency Security Advisor can provide advice on security briefcases.

Where security classified material is removed from the office it must be packaged and stored in accordance with the PSPF. This is to reduce the risk of compromise.

7.9 Audio and photographic equipment

Audio and photographic recording equipment must be afforded the same level of security as other media used to record, process, store or transmit security classified information.

Where this equipment is used, recording tapes, and disks, or the equipment itself (if it utilises on-board digital memory), must be labelled with the protective marking equivalent to the highest level of information recorded therein. The protective marking must be clearly stated at the beginning and end of each recording. Any printed photographic images must have the protective marking labelled appropriately.

Employees conducting meetings or conferences where security classified information is to be discussed, must take necessary precautions to ensure audio and photographic recording equipment is only used for official purposes. This responsibility applies to employees sponsoring visitors to the Agency sites.

7.10 Destruction of classified information

Careless disposal of security classified material increases the likelihood of unauthorised disclosure of information.

Prior to disposal of any electronic equipment which stored FOUO or Sensitive information, the device or electronic storage must be appropriately sanitised so that no traces of the information can be retrieved.

Those records no longer required by the Agency must be disposed of in accordance with approved records (disposal) authorities. The relevant authorities are Agency Records Authority and the General Records Authority – AFDA Express. Both documents are approved by the National Archives of Australia.

No records should be destroyed or transferred as National Archives unless granted prior approval by the agency Records Management area.

In addition to the disposal of formal records using records authorities, Normal Administrative Practice (NAP) can be used to destroy records that have no ongoing value. NAP allows the Agency to

dispose of records without formal authorisation. NAP can be applied to most duplicate, facilitative or other unimportant/short-term reference information (hardcopy or electronic).

Security waste bins ('wheelie style') are provided at Agency sites for the disposal of paper based information up to and including Sensitive material.

The effective disposal of Sensitive waste must consider the following:

- security waste bins must be secured to prevent accidental or deliberate removal of information;
- security waste bins should be cleared regularly to prevent overfilling; and
- removal, transport, storage and destruction must conform to the Agency's security requirements.

Where security waste bins are not available, security classified information must be shredded by the custodian using a Class 'B' cross-cut shredder producing a shred size no greater than 2.3 mm x 25 mm, or a Class 'A' cross-cut shredder producing a shred size no greater than 1 mm x 20 mm.

Keys to security waste bins will not be provided to the individual. Prior to retrieval, the employee will need to provide the attending person with a brief description of the material prior to the bin being unlocked.

Recycling of paper waste is only permitted for Unofficial information or material which has already been shredded by approved methods.

8 Administration and Review of this Guideline

8.1 Review of this Guideline

This guideline will be reviewed **annually** by the Agency Security Advisor for currency and updated if required.

8.2 Administration of this Guideline

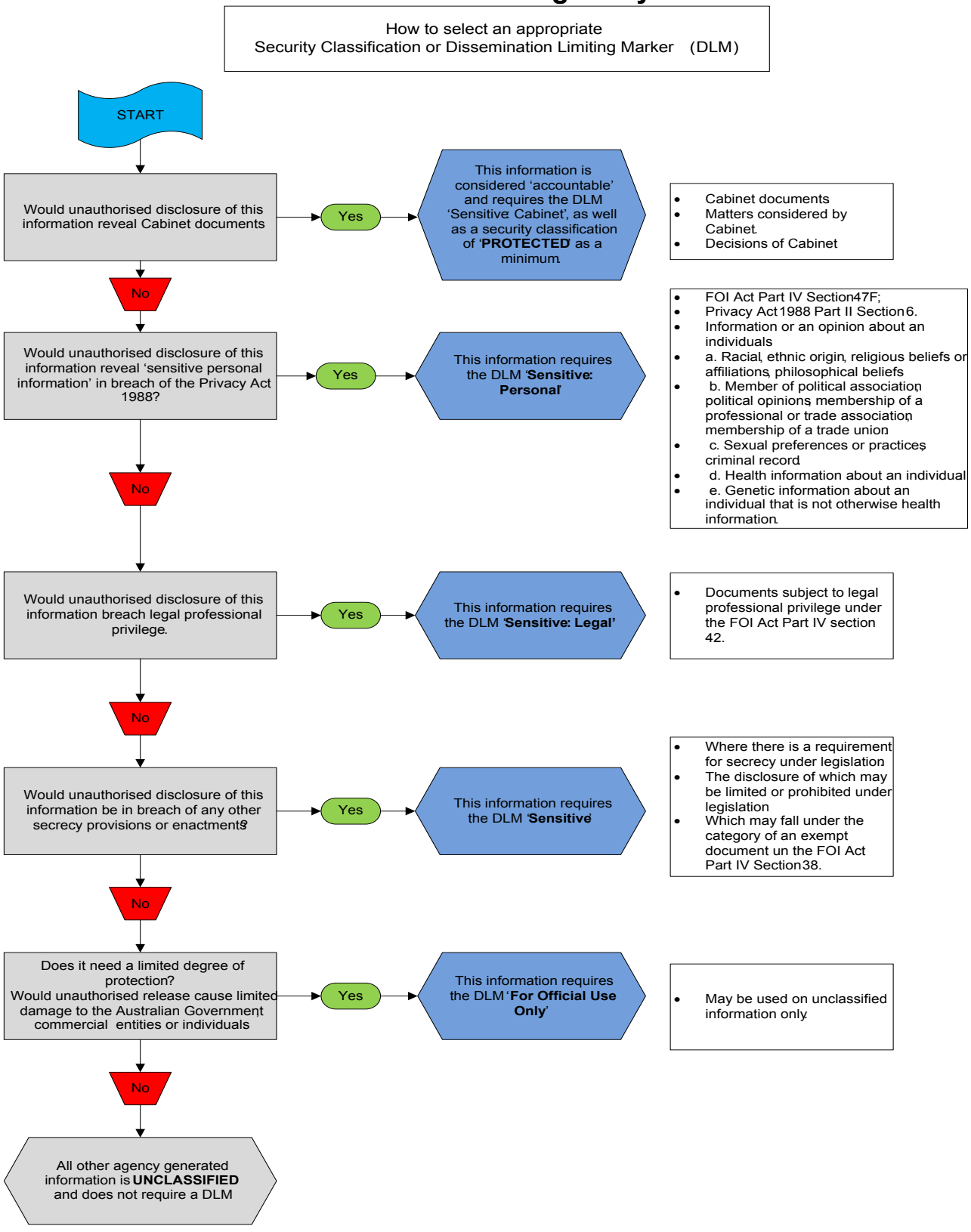
The Agency Security Advisor is responsible for the administration and review of this guideline.

9 Other Documents Applicable to this Guideline

9.1 Applicable Documents

- Agency Security Plan
- Agency Security Policy
- Australian Government Information Security Management Protocol
- Australian Government Security Classification System
- Australian Government Protectively Marking and Handling Sensitive and Security Classified Information
- Information Security Manual
- Information Privacy Principles
- Freedom of Information

Attachment A - Classification and marking ready reckoner chart

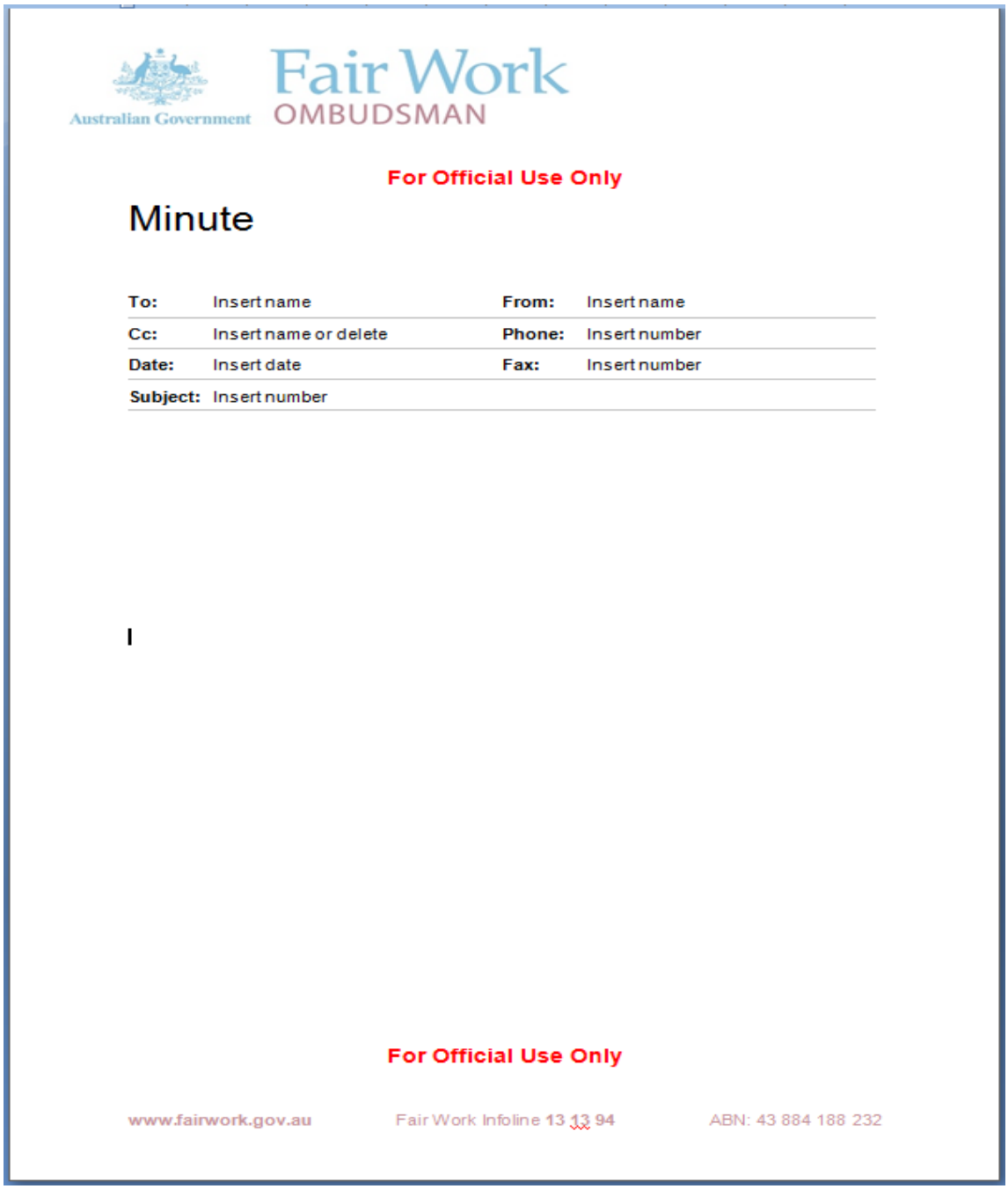


* The DLM 'Sensitive' is only to be used on its own, where the secrecy provisions of enactments may apply, and/or the disclosure of which may be limited or prohibited under legislation.
* When used it is to include a footer on the first page, or separate cover page, referring to the legislative clause/s and relevant secrecy provisions.

Attachment B – Applying a protective marking for DLMs and Cabinet documents

Example 1:

Applying a DLM for **'For Official Use Only'**.



Australian Government Fair Work OMBUDSMAN

For Official Use Only

Minute

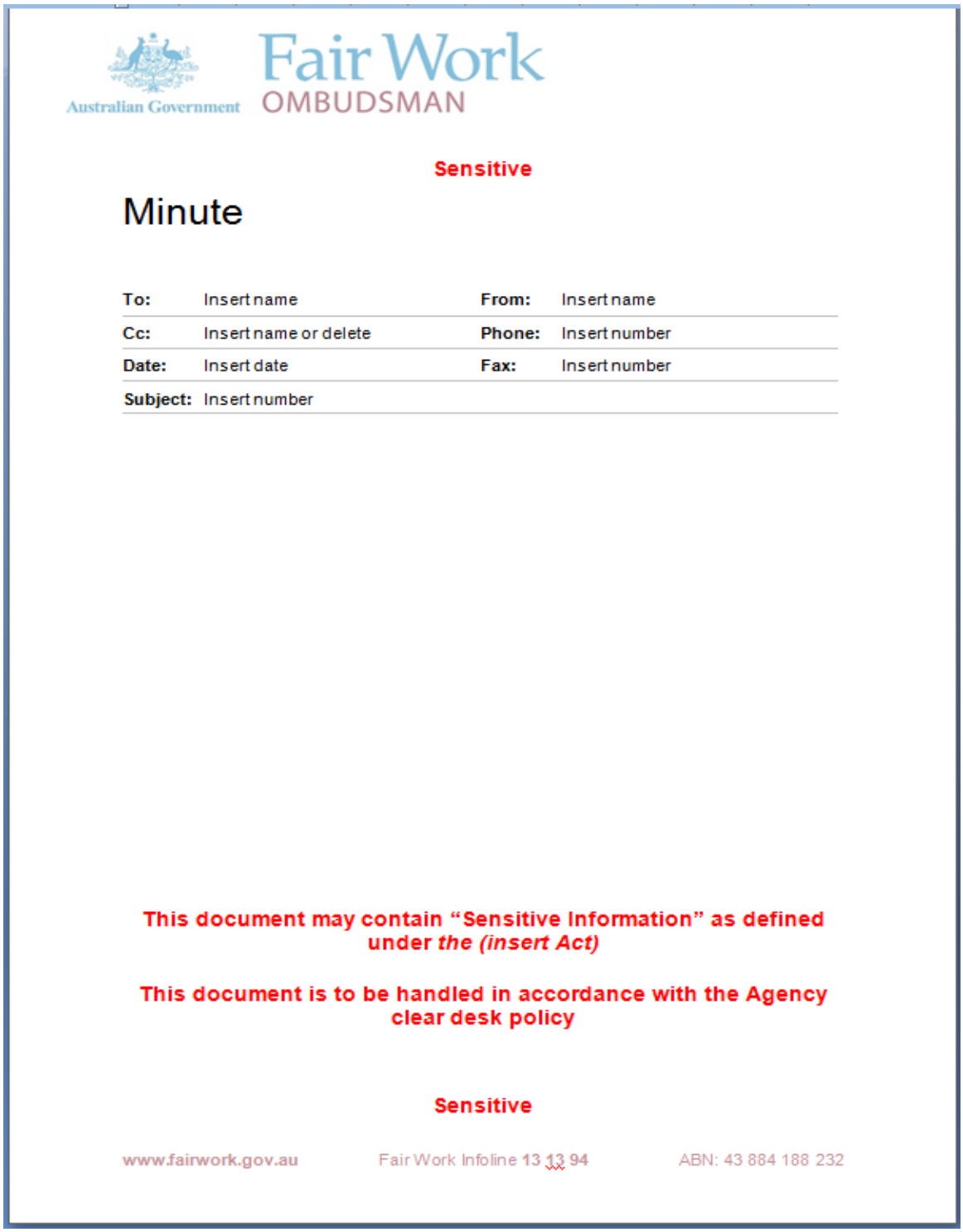
To:	Insert name	**From:**	Insert name
Cc:	Insert name or delete	**Phone:**	Insert number
Date:	Insert date	**Fax:**	Insert number
Subject:	Insert number		

For Official Use Only

www.fairwork.gov.au Fair Work Infoline 13 13 94 ABN: 43 884 188 232

Example 2:

Applying a DLM for '**Sensitive'** must a contain a reason for the marking by referencing the applicable Act.



Australian Government Fair Work OMBUDSMAN

Sensitive

Minute

To:	Insert name	**From:**	Insert name
Cc:	Insert name or delete	**Phone:**	Insert number
Date:	Insert date	**Fax:**	Insert number
Subject:	Insert number		

This document may contain "Sensitive Information" as defined under *the (insert Act)*

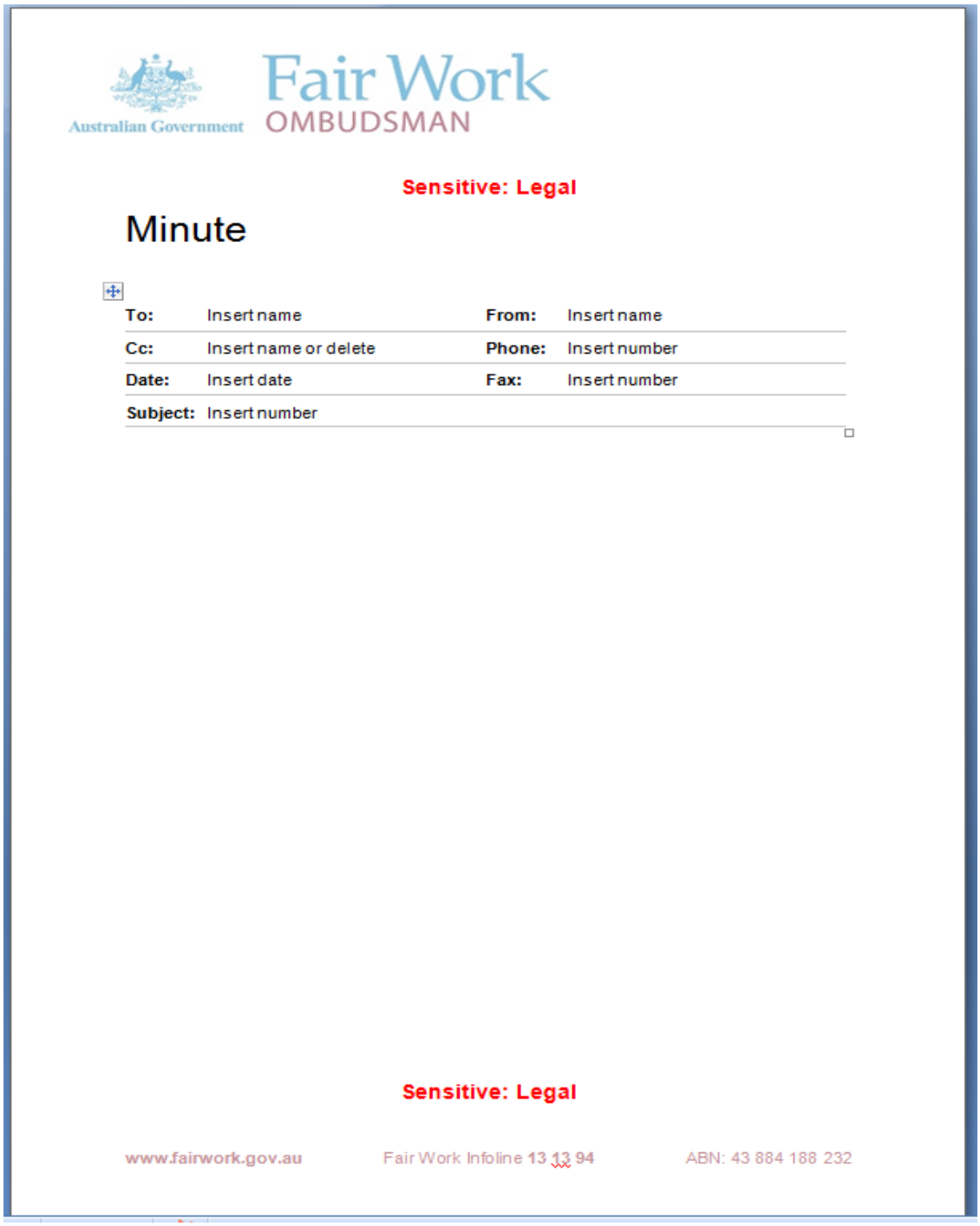
This document is to be handled in accordance with the Agency clear desk policy

Sensitive

www.fairwork.gov.au Fair Work Infoline 13 13 94 ABN: 43 884 188 232

Example 3:

Applying a DLM for '**Sensitive: Legal'** .



Australian Government Fair Work OMBUDSMAN

Sensitive: Legal

Minute

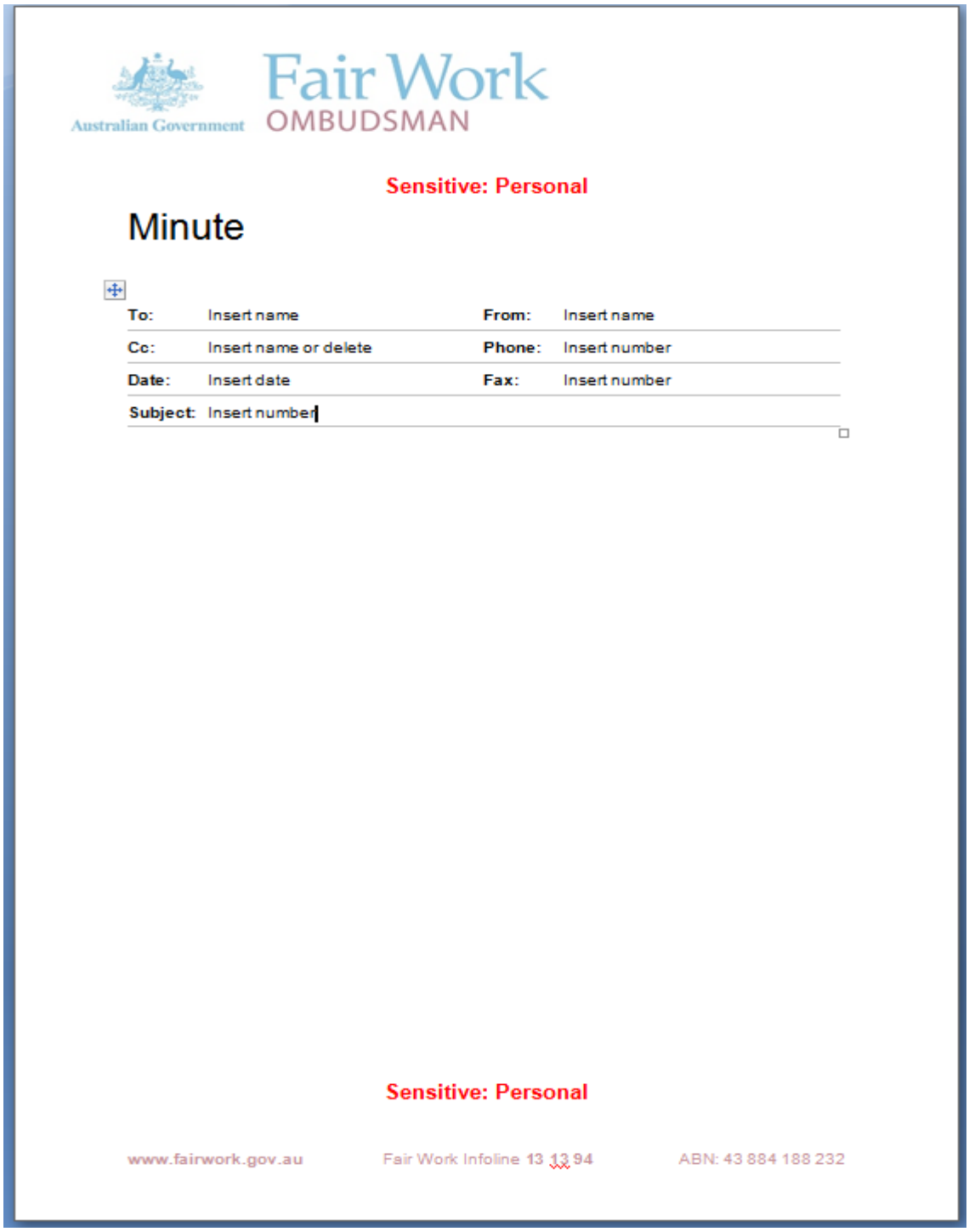
To:	Insert name	**From:**	Insert name
Cc:	Insert name or delete	**Phone:**	Insert number
Date:	Insert date	**Fax:**	Insert number
Subject:	Insert number		

Sensitive: Legal

www.fairwork.gov.au Fair Work Infoline 13 13 94 ABN: 43 884 188 232

Example 4:

Applying a DLM for **'Sensitive: Personal'**.



Australian Government Fair Work OMBUDSMAN

Sensitive: Personal

Minute

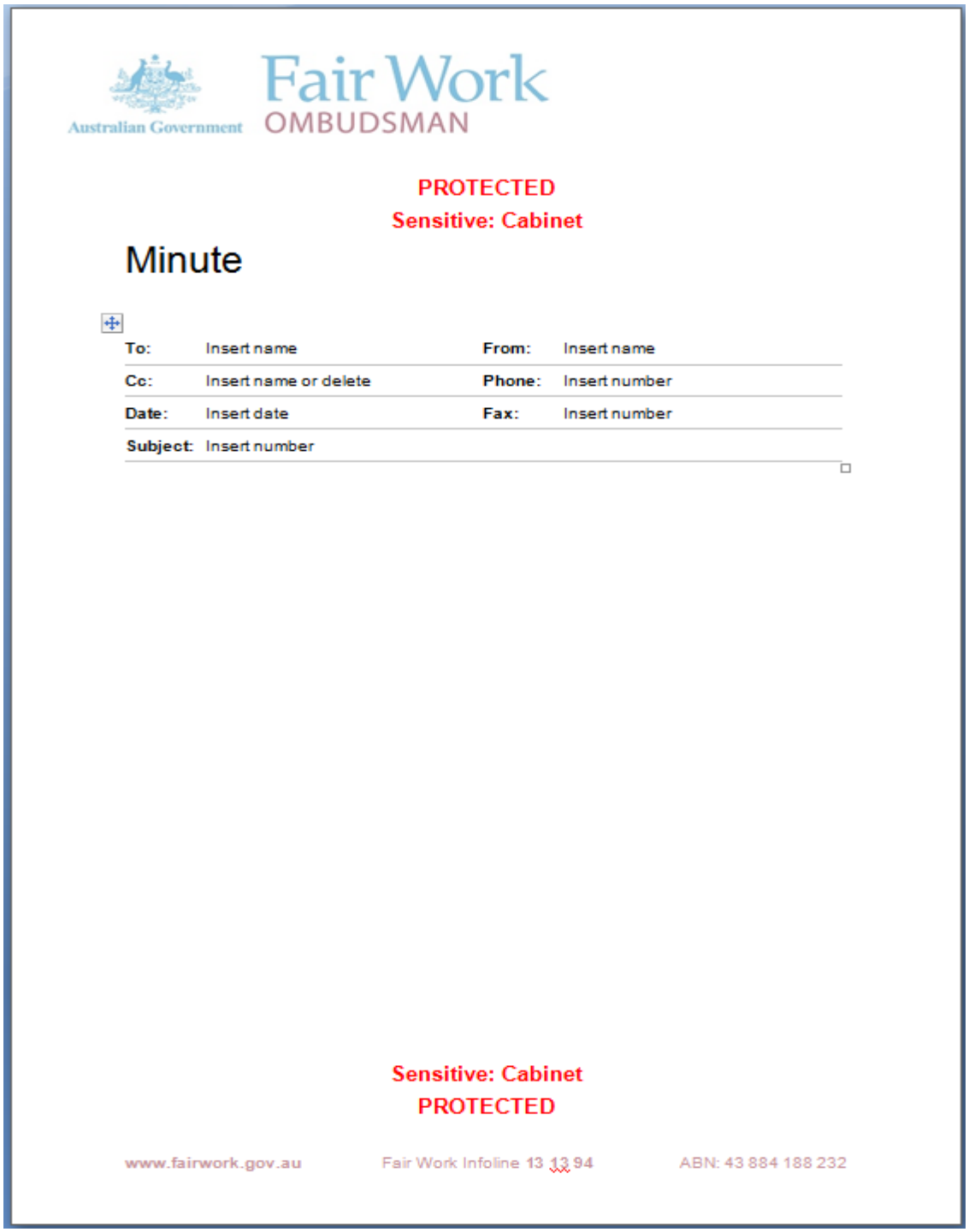
To:	Insert name	**From:**	Insert name
Cc:	Insert name or delete	**Phone:**	Insert number
Date:	Insert date	**Fax:**	Insert number
Subject:	Insert number		

Sensitive: Personal

www.fairwork.gov.au Fair Work Infoline 13 13 94 ABN: 43 884 188 232

Example 5:

Applying a security classification and DLM for Cabinet documents **'PROTECTED Sensitive: Cabinet'**.



Australian Government Fair Work OMBUDSMAN

PROTECTED
Sensitive: Cabinet

Minute

To:	Insert name	**From:**	Insert name
Cc:	Insert name or delete	**Phone:**	Insert number
Date:	Insert date	**Fax:**	Insert number
Subject:	Insert number		

Sensitive: Cabinet
PROTECTED

www.fairwork.gov.au Fair Work Infoline 13 13 94 ABN: 43 884 188 232

Example 6:

TRIM files requiring a cover sheet will contain the following information:

(Insert DLM)

The attached document/s numbered (_) to (_)

Contains information (Insert DLM)

This document is to be handled in accordance with the Agency clear desk policy

(Insert DLM)

Example 7:

TRIM files requiring a cover sheet will contain the following information for Sensitive:

Sensitive

The attached document/s numbered (_) to (_)

May Contain "Protected Information" as defined under the *Fair Work (Building Industry) Act 2012* (FWBI Act)

This document is to be handled in accordance with Agency clear desk policy

Sensitive