ASIC
Australian Securities & Investments Commission

Handling Sensitive and Classified Information - Protocol - 2019

About this protocol

This document assists ASIC staff in determining the appropriate protective marking to apply to information they create as part of their work for ASIC and with the handling controls for sensitive and classified information.

Document Control

Protocol ownership

ASIC Security is responsible for the development and implementation of this protocol.

Protocol application

This protocol applies to all ASIC staff and all official information.

Application of this protocol is subject to approval of the Chief Security Officer (CSO).

Protocol approval

This protocol has been reviewed and approved by the following parties on the following dates:

Version	Approver	Approval date
V1	CSO	

Version history

Version	Details of changes/comments	Date
V1	Consolidates the *Valuing and Handling Classified Information Protocol – January 2016* Incorporates the *Aggregation of Information Protocol – July 2013* Includes the 2018 PSPF reforms to Sensitive and Classified Information Incorporates the *ASIC Printing Policy - July 2019*	October 2019

Distribution

Version	Date	Distribution list
V1	October 2019	All staff via myASIC

Protocol location

This protocol is located on **myASIC** at:

https://ecm.a1.asic.gov.au/shared/myasic/Documents/Security%20Services/PROTOCOL%20-%20Sensitive%20and%20Classified%20Information.pdf

.

Contents

A Protocol Objective

Objective and scope

1. This protocol provides direction to staff on the handling controls and application of protective markings for information and data (information assets) produced and stored by ASIC. The protocol should be read in conjunction with the ASIC Security Management Policy and Plan (SMPP), the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM).

2. Correct protective marking ensures that information assets are handled in accordance with their level of sensitivity, and reduces the risk of inadvertent or unauthorised disclosure or compromise of sensitive or classified material.

3. All staff, contractors and external service providers **must** follow this protocol, which applies to all information assets produced or held by ASIC.

4. This document provides some instruction on the destruction and disposal of information assets. For detailed information on disposal, contact Information and Records Management.

Contacts

5. For advice, please contact ASIC Security, who are also responsible for updating and maintaining this document.

B Why do we protect information?

6. ASIC protects its information assets to maintain its integrity, confidentiality and availability.

7. The information held by ASIC is often sensitive or personal in nature and could be valuable to a wide range of individuals, groups or foreign governments, including:

   a. the media, and private inquiry agents

   b. issues motivated people or groups

   c. organised crime groups or individuals involved in criminal activities

   d. disgruntled, malicious or corrupt employees

   e. members of the public with genuine or perceived grievances against ASIC.

8. The unauthorised or accidental release of information may cause harm to an individual, ASIC, the Government or a commercial entity.

C Assets and Records

Information assets

9. The term 'information assets' within these guidelines refers to any form of official information, including:

   a. electronic data

   b. software or ICT systems, removable devices and/or networks on which the information is stored, processed or communicated

   c. printed documents and papers

   d. the intellectual information (knowledge) acquired by individuals

   e. physical items from which information regarding design, components or use could be derived.

10. All information created as part of your work for ASIC and the Government is official information and is a record of what you have done. Information assets must be assessed for sensitivity and labelled with a protective marking at the point of introduction into the ASIC environment, whether the information asset has been generated, received, or procured.

Systems used to maintain ASIC records

11. ASIC records must be stored in an authorised recordkeeping system, e.g. SharePoint ECM or CRM. Records created when using hosted web services, social media applications or mobile devices **must** be captured in an authorised ASIC recordkeeping system.

12. Contact Information and Records Management for advice on appropriate storage of ASIC records including Software as a Service and outsourced service arrangements.

D Responsibilities

If you are the:	Then your responsibility is:
Information Author (Originator) / User	• Determining and applying the appropriate sensitivity or security classification to information you create • Ensuring that records are properly maintained for the matters for which you are responsible. This includes the creation, maintenance and disposal of ASIC's records • Adhering to the processes outlined in this protocol and complying with the SMPP, PSPF and ISM • Capturing records into an authorised ASIC recordkeeping system to provide evidence of the actions, decisions and communications • Seeking advice from Information and Records Management if unsure of your recordkeeping requirements or responsibilities • Contacting ASIC Security if you: o are unsure about protective markings o suspect a breach of policy relating to information handling and classification.
System Owner	• Maintaining technology for ASIC information and recordkeeping systems under your ownership, including maintaining appropriate system accessibility, security and business continuity measures • Ensuring that any actions, such as removing data from systems or folders, are undertaken in accordance with these guidelines and the *National Archives Act*.
Information Manager	• Providing training, advice and general support to all staff. • Developing, implementing and maintaining records management products and tools, including systems, to assist in the creation of complete and accurate records • Promulgating ASIC information and records management policies and guidelines to all staff • Monitoring staff and systems compliance • Ensuring that records are retained in accordance with the *National Archives Act*.

E What is protective marking?

Protective markings

12. Protective markings provide staff with a visual aid to inform the reader how to handle (store, copy, etc.) and who can access the information.

13. The correct application of protective markings is designed to protect the integrity, confidentiality and availability of official information.

14. The Government updated the sensitive and classified information protective marking scheme in 2018. The new markings that Government agencies **must** use are:

Protective Marking	Category of Information
OFFICIAL	Business as usual
OFFICIAL: Sensitive	Sensitive business as usual
PROTECTED	Security classified information
SECRET	
TOP SECRET	

15. Anything you create as part of your work for ASIC is official information, so the OFFICIAL marking, whilst not mandatory, is the default setting. A document or data file that does not display a protective marking is therefore deemed OFFICIAL.

16. If you believe the information you create requires additional security or handling requirements, for example it might contain price sensitive information, you should indicate this by applying the OFFICIAL: Sensitive marking.

17. If you believe compromise or unauthorised access to the information you create may, for example, lead to a potentially life-threatening injury to an individual or substantially impact the national economy then you should apply the national security classification of PROTECTED.

18. Staff **must** be mindful of not over-classifying information that they create, as this limits with whom the information can be shared.

19. Staff **must not** change the protective marking of information received from an external agency, or information created by a different ASIC business unit, without written permission from the author / originator.

Information limiting markers

20. Additional Information Limiting Markers (ILM) are available for use with the **OFFICIAL: Sensitive**, **PROTECTED**, **SECRET** and **TOP SECRET** protective markings. The ILMs further assist staff in recognising information that requires additional handling controls and security. These are:

Information Limiting Marker
Commercial [1]
Legal privilege [2]
Legislative secrecy [3]
Personal privacy [4]
For example
OFFICIAL: Sensitive: Commercial
PROTECTED: Personal privacy

[1] Restrictions on access to, or use of, business information that could compromise ASIC's or another party's commercial interests.
[2] Restrictions on access to, or use of, information covered by legal professional privilege.

[3] Restrictions on access to, or use of, information covered by legislative secrecy provisions, e.g. certain sections in the *Crimes Act 1914*, *Criminal Code Act 1995* and the *Taxation Administration Act 1953*.

[4] Restriction, under the *Privacy Act 1988*, on access to, or use of, personal information collected for business.

F Determining the appropriate protective marking

Information assets

21. The PSPF sensitive and classified information system identifies and establishes the access and handling requirements for information, and the potential impact due to unauthorised disclosure, accidental or deliberate misuse or modification, loss or damage.

22. Information that requires a protective marking must be handled in accordance with that marking.

23. The following tables outline the protective markings and parameters required for their application to information, resources and assets:

Category	Protective Marking	Types of Information	Parameters
BAU information	OFFICIAL	The types of information that would typically be labelled **OFFICIAL** could include: • internal policies • procedural documentation • guidelines for employees • training material.	ASIC Information that is not sensitive, but requires safeguards to prevent unauthorised access, tampering or public release is referred to as **OFFICIAL** information. Previously, this information was marked Unclassified. The new marking, **OFFICIAL**, replaces Unclassified • information marked as '**OFFICIAL**' will be treated in the same manner as information currently marked as Unclassified, or not marked at all o only information that is designated '**OFFICIAL**' is appropriate for general public release **Note (i): Do not use with material labelled as 'Cabinet'** **Note (ii): The UNOFFICIAL marking is for use with personal non-work-related information.**

Category	Protective Marking	Types of Information	Parameters
Sensitive BAU information	**OFFICIAL: Sensitive**	Most of the ASIC sensitive information or data warrants the **OFFICIAL: Sensitive** protective marking. Examples include: • audit reports, including many internal audit reports • sensitive internal documents and reports, for example relating to investigations, risk assessments, sensitive proposals • any information relating to individuals or organisations which contains personal identifying details or commercially sensitive information • any information relating to staff which contains personal identifying details • tender responses to ASIC contracts and other information supplied in an expectation that it will be treated as commercial-in-confidence • IT system-related information that could cause harm if exploited or misused.	The **OFFICIAL: Sensitive** protective marking replaces the previous markings of: For Official Use Only or FOUO, Sensitive, Sensitive: Legal, and Sensitive: Personal It is used when compromise of the information could reasonably cause limited damage to the Australian Government, commercial entities, or members of the public Examples of limited damage include: • limited distress to individuals or private entities, including through breach of privacy or damage to reputation • financial loss or loss of earning potential, or facilitate improper gain or advantage, to individuals or private entities • prejudice the investigation or facilitate the commission of crime • breach proper undertakings to maintain the confidentiality of information provided by third parties • impede the effective development or operation of Government policies • breach statutory obligations regarding the management and disclosure of information • disadvantage the Government in commercial or policy negotiations with others • undermine the proper management of the public sector and its operations. **Note: Do not use with material labelled with 'Cabinet'.**

Category	Protective Marking	Types of Information	Parameters
Security classified information	**PROTECTED**	Examples of the types of information that may attract the **PROTECTED** classification within ASIC include: • s 47E (d) [redacted] • [redacted] • [redacted] • [redacted] • [redacted] • [redacted]	Information classified as **PROTECTED** requires a substantial degree of protection, as its unauthorised release could reasonably cause damage to the Australian Government, commercial entities, or members of the public It is to be used in specific circumstances, for instance, when compromise of the information could: • endanger individuals or private entities • work substantially against national economy or commercial interests • substantially undermine the financial viability of major organisations • seriously impede the development or operation of major Government policies • prejudice the investigation or prosecution or facilitate the commission of serious crime.

Category	Protective Marking	Types of Information	Parameters
Security classified information	SECRET	Only very limited security-classified information warrants this protective marking. s 47E (d) [redacted] [redacted]	s 47E (d) [redacted] Contact ASIC Security if you believe your work touches this level Information that requires a significant degree of protection, where the unauthorised release could reasonably result in serious damage to the Australian Government, commercial entities, or members of the public Its use must be limited **only** to circumstances where compromise of the information could: • directly threaten life • seriously prejudice public order • substantially damage national finances or economic and commercial interests.

Category	Protective Marking	Types of Information	Parameters
Security classified information	TOP SECRET	If you believe you are required to create, store or handle any information at TOP SECRET, you must contact ASIC Security.	s 47E (d) [redacted] Information that requires classification at the TOP SECRET level requires the highest degree of protection available. There are extremely limited circumstances where this will be required within ASIC If you believe you need to create, discuss or receive information at the TOP SECRET level, contact ASIC Security in the first instance.

G Limiting access to sensitive and classified information to those who need to know

Rationale

24. The Government expects agencies to keep classified information to a minimum. Most of the information created at ASIC should therefore only require the **OFFICIAL: Sensitive** marking.

25. The Government mandates that access to, and dissemination of, sensitive and security classified information is limited to personnel who need the resources to do their work. This involves:

    a. providing access to information only to personnel who need that access; not based on convenience or because of their status, position, rank or level of authorised access

    b. a positive obligation to share relevant information so that people with an operational need to know the information have access.

26. In addition to having an operational / genuine need-to-know, ASIC must limit access to security-classified information to those with the necessary security clearance.

27. The security clearance level for access to information classified as **PROTECTED** is Baseline or higher.

Considerations

28. Staff **must** consider the amount of harm [5] that the unauthorised release of any information would cause when applying a protective marking.

29. Staff **must not** use a security classification to prevent other staff from accessing information because an investigation is confidential, etc. In such circumstances s 47E (d) [redacted].

30. Staff **must not** use a security classification to avoid release under a Freedom of Information application.

[5] 'Harm' requiring information to be classified as PROTECTED is defined as:
"damage to an individual such as discrimination, mistreatment, humiliation or the undermining of an individual's dignity or safety that leads to potentially significant harm or potentially life-threatening injury.
or
Damage to ASIC's operations to an extent and duration that ASIC cannot perform one or more of its primary functions".

31. Information that is marked as OFFICIAL (**insignificant damage**) or OFFICIAL: Sensitive (**limited damage**) can be provided to external non-Government people (including members of the public) where there is a genuine need to know and there are no legislative barriers to releasing the information.

32. If the compromise of official information may result in **damage** to an individual, organisation or Government, then the author / originator must assess the information as PROTECTED.

33. The need-to-know principle applies to all sensitive and classified information. It reflects the need for staff to access this information only where there is an operational requirement to do so. The practice helps personnel understand their responsibility to protect information, including the correct methods for storage, handling and dissemination.

34. Over-classifying your information creates unnecessary restrictions that staff **must** adhere to, for example, s 47E (d) [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

H Control and handling of official information

35. The following tables relate to the handling of official information and assets, including sensitive and security classified information, and how they apply broadly to ASIC. Staff should always refer queries to ASIC Security if they are unsure of handling or classification procedures.

OFFICIAL	
Access requirements	• s 47E (d) [redacted] • Need-to-know.
Minimum storage requirements	• ASIC IT network (digital) • s 47E (d) [redacted] • Clean desk and locked screen when away from your desk.
Marking	• Best practice • Centred top and bottom of each page • OFFICIAL • Page numbers.
Printing & Copying	• Permitted on the ASIC IT network and follow-me-printing, in accordance with the person's duties.
Emailing	• Email to a non-dot gov dot au address is permitted.
Transfer within an ASIC office	• Permitted, in accordance with the person's duties.
Transfer between ASIC offices or to other Government agencies	• Permitted, in accordance with the person's duties, e.g. for meetings • Information may be used for home-based work in accordance with the person's duties.
Audit & Destruction	• No audit requirements • Once a record is created it cannot be destroyed unless in accordance with the Archives Act • Shredding or via secure document destruction bins.

OFFICIAL: Sensitive	
Access requirements	• s 47E (d) [redacted] • Need-to-know.
Minimum storage requirements	• ASIC IT network (digital) • s 47E (d) [redacted] • Clean desk and locked screen when away from your desk.
Marking	• Mandatory • Centred top and bottom of each page • **OFFICIAL: Sensitive** • Page numbers.
Printing & Copying	• Permitted on the ASIC IT network and follow-me-printing, in accordance with the person's duties.
Emailing	• Email to a non-dot gov dot au address is permitted • Sender **must** confirm recipient's email address **before** sending
Transfer within an ASIC office	• Permitted, in accordance with the person's duties.
Transfer between ASIC offices or to other Government agencies	• Permitted, in accordance with the person's duties, e.g. for meetings • Information may be used for home-based work in accordance with the person's duties but **must** be secured from unauthorised access when not in use.
Audit & Destruction	• No audit requirements • Once a record is created it cannot be destroyed unless in accordance with the Archives Act • Shredding or via secure document destruction bins.

Aggregated value of OFFICIAL: Sensitive information

36. Whilst each single piece of information requires a protective marking and appropriate handling, sometimes the aggregated value of a significant volume of information increases the collective value of the information. Where this occurs, the sensitivity value for the container in which the information is stored increases and the container should be marked PROTECTED.

37. If you have a significant volume of information or data assets marked as OFFICIAL: Sensitive, contact ASIC Security for guidance.

Reclassification

38. Reclassifying information refers to both the downgrading and upgrading of a security classification when the sensitivity of the information changes. The same principles and considerations apply to reclassification as to initial classification.

39. The reclassification of information **must** only be performed by, or in consultation with, the Information Owner or their SEL / ED. This includes information provided by an external agency.

40. If the originator is no longer with ASIC, then the confirming authority is either the SEL of the business unit where the information originated or the Chief Security Officer (CSO) through the ASA.

41. When information is reclassified, all known copies of the information should be updated to reflect the new protective marking. This may involve contacting other agencies where reclassified material has been distributed outside ASIC.

42. Historical classified information should be reviewed to assess whether it still requires the classification and should be declassified, if appropriate.

43. Please contact ASIC Security and Records management to de-classify your previously over classified material.

I How to apply a protective marking

44. The following instructions guide staff through the process of applying a protective marking to ASIC information.

45. Where possible, the protective marking should be in bold upper-case text with a minimum height of 5 millimetres, at the centre top and bottom of each page.

46. If, for practical and/or operational security reasons, it is necessary to implement a non-textual labelling scheme, the procedure must have documented approval from the Chief Security Officer, via the Agency Security Adviser.

Media Type	Labelling Method
Documents	The protective marking **must** be applied at the top and bottom of each page, in bold upper-case text with letters at least 5mm high as highlighted in Figure 1.
Information or media with covers (such as books, pamphlets, reports, CDs and DVDs)	**Must** show the protective marking on the front cover, title page, and rear cover. Any bindings or fastenings **must not** obscure the protective marking. Where security-classified information or media are filed, the security classification must be clearly visible (for example, along the spine of a lever-arch file).
Emails	The pop-up box in Outlook for emails **must** be used to apply the protective marking before the email can be sent. The protective marking **must** be the same as the highest level of any attachment to the email.
Servers and Hard Drives	**Must** clearly show the protective marking on the top or front covers.
Tape Media	All backup tapes **must** be labelled with a protective marking.
Other Portable Media (e.g. USB devices)	The protective marking **must** be applied on the device in a place that is easily visible.

48. The following image provides guidance on how markings should appear on documents. In this example, optional paragraph markings are used to indicate where the sensitive material is included.

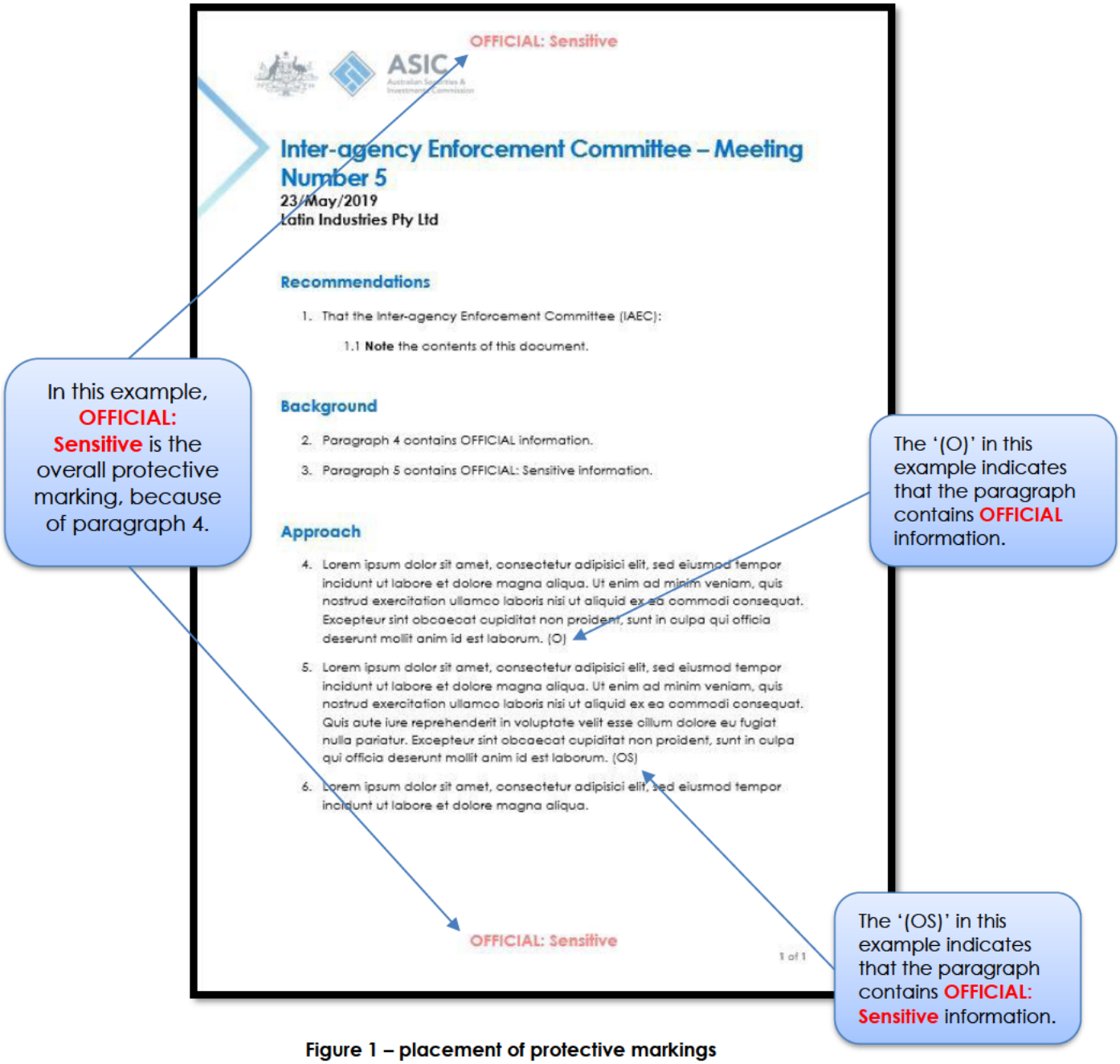

Figure 1 – placement of protective markings

J Managing information received by ASIC

49. ASIC **must** protect all information it receives from an external agency, stakeholder, customer or subject of an investigation.

External Australian government agency information

50. If staff receive information from an external agency, e.g. AUSTRAC, ACIC or the AFP, that already displays a protective marking, ASIC staff:

a. **must not** alter that marking unless expressly authorised, in writing, by the parent agency

b. **must not** further disseminate the information unless permitted by the MOU or agreement

c. **must** contact the parent agency if their information is captured by a production notice or FoI request etc.

External Australian government agency information - caveats

51. If staff receive caveated information from an Australian government agency, ASIC staff:

a. **must not** provide **AUSTEO** (Australian Eyes Only) marked information to non-Australian citizens (including staff holding citizenship waivers)

b. **must not** provide **AGAO** (Australian Government Access Only) marked information to non-Australian government employees

c. **AGAO** information is releasable to foreign staff on secondment and staff holding citizenship waivers

d. **must not** release information marked **REL/** [country abbreviations, e.g. AUS/CAN/USA] to citizens from countries not listed.

Foreign government agency information

52. If staff receive information from a foreign government agency, ASIC staff:

a. **must** handle the information in accordance with the MOU, International Agreement or International Arrangement in place with the country providing the information

b. **must not** alter that marking unless expressly authorised, in writing, by the foreign government agency

c. **must not** further disseminate the information unless permitted by the MOU, Agreement or Arrangement

d. **must** contact the foreign government agency if their information is capture by a production notice, etc.

Communications service provider information

53. In many cases the information obtained from other providers may only be used for ASIC's intelligence purposes and staff are not permitted to disclose it.

54. ASIC staff:

a. **must** obtain a court statement, through the Intelligence Support team if the information will be used for evidentiary purposes

b. **must** seek legal advice from the CLO to determine whether information may be obtained in the circumstances of a case and whether there are special restrictions in the way information obtained may be used or disclosed (including for court)

c. **must** apply the protective marking of **OFFICIAL: Sensitive** to the information.

Information provided pursuant to the *Australian Securities and Investments Commission Act 2001*

55. ASIC must take all reasonable measures to protect information provided under the Australian Securities and Investments Commission Act 2001 Sections during a hearing or in response to a summons, from unauthorised use or disclosure.

a. for most information, staff should apply the protective marking of **OFFICIAL: Sensitive**

b. for information that would disclose the identity of a whistle-blower and may place them in danger, staff should consider applying the classification of **PROTECTED**.

K Printing and copying sensitive and classified information

56. All ASIC printers and multi-function devices (MFD) are managed by ASIC IT and are suitable for printing and scanning information up to and including the level of PROTECTED.

57. Staff **must not** print, photocopy or scan a document marked as SECRET or TOP SECRET on an ASIC network MFD, personal or stand-alone printer.

ASIC Secure-printing

58. ASIC employs 'secure-printing' which allows auditable and consistent printing, scanning and copying throughout all ASIC sites.

59. All staff **must** authenticate at the printer or MFD with their building access pass to retrieve print jobs. Print jobs that have not been printed will be automatically deleted from the print queue after 17 hours.

60. As secure printing will not print any documents until a user has authenticated to a printer, staff **must** ensure that they collect ALL documents at the conclusion of the print job.

61. Staff **must not** leave the MFD unattended during operation and **must** ensure that they log-off from the MFD at the conclusion of the print job.

62. Requests for a personal MFD **must** outline the exceptional circumstances and be approved by:

    a. SEL – Corporate Services, then

    b. Chief Information Officer, then

    c. Chair of the Digital Governance Sub-Committee.

63. All ASIC printers and MFDs are to set to print double-sided by default.

L Remote Working

64. The sensitive and classified information handling requirements are driven by the labels and remain same either working from office or working remotely.

65. Team member who removes official information from an ASIC facility or prints official information at home becomes responsible for handling the information in accordance with the minimum protections for the label and ensure it is returned to ASIC for appropriate disposal.

66. Team members should not send ASIC documents to their personal email address for printing.

67. Approved personal MFDs should provide a print log if requested.

68. While working remotely, the information should be stored as defined by the sensitive and classified labels.

69. All ASIC team members should remain aware of who is present within the remote working environment. All team members must:

    a. prevent their computer screens from being read by people not employed by ASIC.

    b. take all reasonable precautions to prevent official conversations being overheard by people not employed by ASIC.

    c. Maintain the confidentiality from other house mates and / or family.

SECRET and SECRET: Cabinet	
Remote Working	• Contact ASIC Security
TOP SECRET and TOP SECRET: Cabinet	
Remote Working	• Contact ASIC Security

M Historical classifications and sensitivity markings

70. There are several historical security classifications and other protective markings no longer reflected in Australian Government policy. The table below outlines the most recent changes that occurred on 1 July 2018. In some cases, equivalencies have been established with current sensitive or classified information levels. Back-capturing of existing information is not required.

Historical Classification or Sensitive Marking	Current Sensitive or Classified Information Level Equivalency	Handling of Historical Markings
CONFIDENTIAL	None	Unless otherwise re-classified, treat as PROTECTED
For Official Use Only (or FOUO)	FOUO is equivalent to the current **OFFICIAL: Sensitive** level	As per requirements for OFFICIAL: Sensitive information
Sensitive	Unless otherwise classified, Sensitive is equivalent to the current **OFFICIAL: Sensitive** level	• If classified, as per the identified classification level; or • If not otherwise classified, as per requirements for OFFICIAL: Sensitive information.
Sensitive: Legal	Unless otherwise classified, Sensitive: Legal is equivalent to the current **OFFICIAL: Sensitive** level	• If classified, as per the identified classification level; or • If not classified, as per requirements for OFFICIAL: Sensitive information.
Sensitive: Personal	Unless otherwise classified, Sensitive: Personal is equivalent to the current **OFFICIAL: Sensitive** level	• If classified, as per the identified classification level; or • If not classified, as per requirements for OFFICIAL: Sensitive information.

N Additional information

The following documents provide staff with further information about information labelling.

Protective Markings – Comparison to previous scheme
Employee Guide – Protective marking of sensitive and classified information
PSPF – Core Requirement 8 – Sensitive and classified information
PSPF – Core Requirement 9 – Access to information