Australian Government
Defence

Defence Security

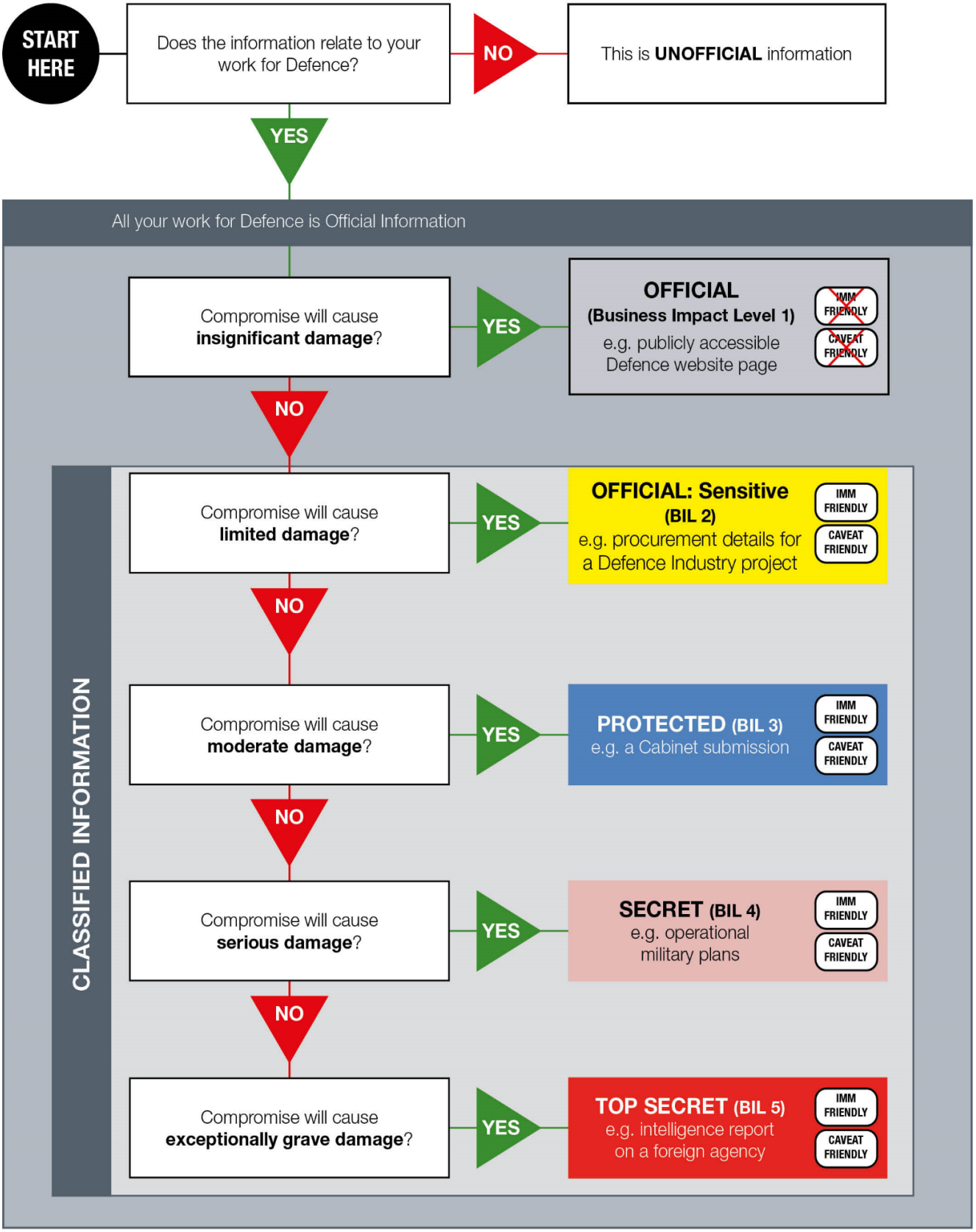
Guide to Assessing and Protecting Official Information

Quick Reference Guide

to Assessing and Protecting Official Information

Use this chart to assess and apply the appropriate level of protection to your information

Further guidance can be found in the Australian Government - Security Caveat Guidelines



Damage Level

Level	Could cause:	Business Impact to Defence	Protection
None	· No damage	None	**UNOFFICIAL** Page 9
Insignificant	· Minor issues for routine business operations and diplomatic activities · Minor impact to Defence assets or budget · No issues with legislation, commercial confidentiality or legal requirements	Low	**OFFICIAL** Page 10
Limited	· Defence's business functions to weaken · $10m to $100m damage to Defence assets · Minor loss of confidence in government · Suffering, harm or injury to someone, but not endanger their life	Low to Medium	**OFFICIAL: Sensitive** Page 12
Moderate	· Disruption to one of Defence's main functions · $100m to $10b damage to Defence assets or budget · Major loss of confidence in government · Suffering or life threatening injury	High	**PROTECTED** Page 14
Serious	· The disruption of all Defence functions · Prevention of major policies · Financial damage to an Australian industry sector · Suffering and loss of life	Extreme	**SECRET** Page 16
Exceptionally grave	· The collapse of political stability in Australia · The collapse of the Australian economy · The collapse of all major national infrastructure · Widespread suffering and loss of life	Catastrophic	**TOP SECRET** Page 18

Caveats

CAVEAT FRIENDLY

A caveat identifies information that requires additional special protection.
Use an additional caveat marker, (e.g. CABINET, AGAO, AUSTEO), if your information contains the following:

Special handling instructions (Including CABINET)
Releasability caveats (AGAO, AUSTEO)
Sensitive compartments (Codewords)
Foreign government markers.

See **page 23** for more information about caveats.

IMMs

IMM FRIENDLY

Information Management Markers

If your information contains legal, legislative or personal details, you may require one of the following Information Management Markers (IMM) to share your information accurately with the right people:

- Legal privilege
- Legislative secrecy
- Personal privacy.

See **page 22** for more information about IMMs.

Introduction

Information security has never been more important to Defence's ability to achieve our mission to defend Australia and its national interests in order to advance Australia's security and prosperity. The work we do in Defence is unique and in many cases classified. We engage with the nation's most sensitive issues and our capability edge relies on us all protecting sensitive information and systems.

In this information age, we face more sophisticated, well-resourced and more capable attacks and threats to our systems, assets, materials and information. All personnel play a role in securing Defence to maintain our capability edge.

Whether you work in Defence or with Defence, you are accountable for ensuring Official Information is treated with the highest level of integrity, accountability and security.

This guide will help you understand how we use protective security markers to protect our Official Information. It also identifies your role and responsibilities to protect our Official Information, how to mark or classify information appropriately, what each marker means and what to do if the information becomes compromised.

All Defence and Defence Industry personnel are encouraged to use the guide and ensure all our information remains secure now, and into the future.

Defence Security – Guide to Assessing and Protecting Official Information
Version 5.0 2025

Contents

Why do we need to protect Official Information?

Information security allows Defence to share and exchange information with confidence. It ensures a common understanding of confidentiality requirements and the consistent application of protective security measures.

A key priority for Defence security is to prevent the unauthorised disclosure of information. Hostile activity against the Australian Government, Defence industry and private sector systems continues to increase.

Australian information is a target because of our:

- strategic position and alliances
- leadership in science and technology
- industrial capability, workforce and resources.

At its most serious, compromised information can damage Australia's international security reputation and put the lives of Australians at risk.

Assessing Information

When you create information, you are best positioned to:

- assess the sensitivity of the information
- apply the appropriate marker or classification
- protect the information appropriately.

When you are assessing information, you are thinking about how much damage the information could cause Defence, if it was compromised.

Ask yourself the following questions:

- How sensitive is the information?
- Who is going to receive or access this information?
- What damage will it do if it is compromised?
- If you over-classify the information, could a military operation fail if the information is needed urgently?

Appropriate Protection

Appropriate access to Official Information enables Defence to operate effectively and efficiently. This can be significant when information sharing is required with other countries or agencies.

You must assess the information each and every time before applying a protective marker.

Understanding *Need-to-Know*

Your work for Defence must only be shared with those who need to know the information for their official duties. This is called the *Need-to-Know* principle.

Protecting information appropriately

Information security markers and classifications allow Defence to share and exchange information with confidence. It is a well-known system, which enables the consistent application of protective security measures.

When you mark information with a protective marker or classification, you are identifying how sensitive or important the information is. You are indicating who should have access and how the information must be handled.

There are several ways you can identify and protect Official Information including:

- Information Management Markers
- Caveats
- Classifications.

There are now six levels of protective markers and classifications:

- UNOFFICIAL
- OFFICIAL
- OFFICIAL: Sensitive
- PROTECTED
- SECRET
- TOP SECRET.

Security Information Overview

UNOFFICIAL	UNOFFICIAL Information is not related to your work at Defence. You are not required to keep a record of this information.

OFFICIAL			OFFICIAL Information includes all your Defence business activities and information, including: • hand written notes that you write at a Defence meeting • an email to a work colleague about a Defence matter • information prepared for public access or circulation, such as websites or Frequently Asked Questions.		
OFFICIAL: Sensitive	▶	**Security caveats** Caveats used for PROTECTED and above: · CABINET · EXCLUSIVE FOR · AUSTEO · AGAO · Releasable to. Apply caveats to manage the access and use of information.	Information classified as OFFICIAL: Sensitive containing sensitive data that could impact Defence functions or the safety and reputation of an individual. Information could include: • a medical report about a Defence member • commercial data that, if compromised, would undermine an Australian organisation or company.	◀	**Information Management Markers** If your information contains legal, legislative or personal details, you may require one of the following IMMs to share your information accurately with the right people: · Legal privilege · Legislative secrecy · Personal privacy.
PROTECTED	▶		Information classified as PROTECTED would be expected to cause damage to national interests, organisations or individuals. Its unauthorised access or release could cause: • a major loss of confidence in the Government • the exposure of discussions or decisions of Cabinet.	◀	
SECRET	▶		Information classified as SECRET is valuable, important and sensitive material. Its unauthorised access or release could cause: • exposure about current military movements • a direct threat to the internal stability of Australia • undermining people's safety that could lead to the loss of life of an individual or small group.	◀	
TOP SECRET	▶		TOP SECRET is the most valuable and sensitive information and carries the highest classification. Its unauthorised access or release could cause: • a compromise of intelligence involving a foreign government • collapse of the political stability of Australia • widespread loss of life.	◀	

Damage

Defence uses Business Impact Levels (BILs) to help you consider and identify the potential damage unauthorised release of your information could cause to people, organisations or government. You can refer to Principle 10 of the *Defence Security Principles Framework* (DSPF) Classification and Protection of Official Information, for more information about BILs.

Unauthorised access or release of Official Information

Report any unauthorised access or release of Official Information to your Security Officer, commander or manager.
A Security Report will also be required.

Changes to the Classification System

The Commonwealth's *Protective Security Policy Framework* (PSPF) updated Australia's protective markers and classifications in October 2018.

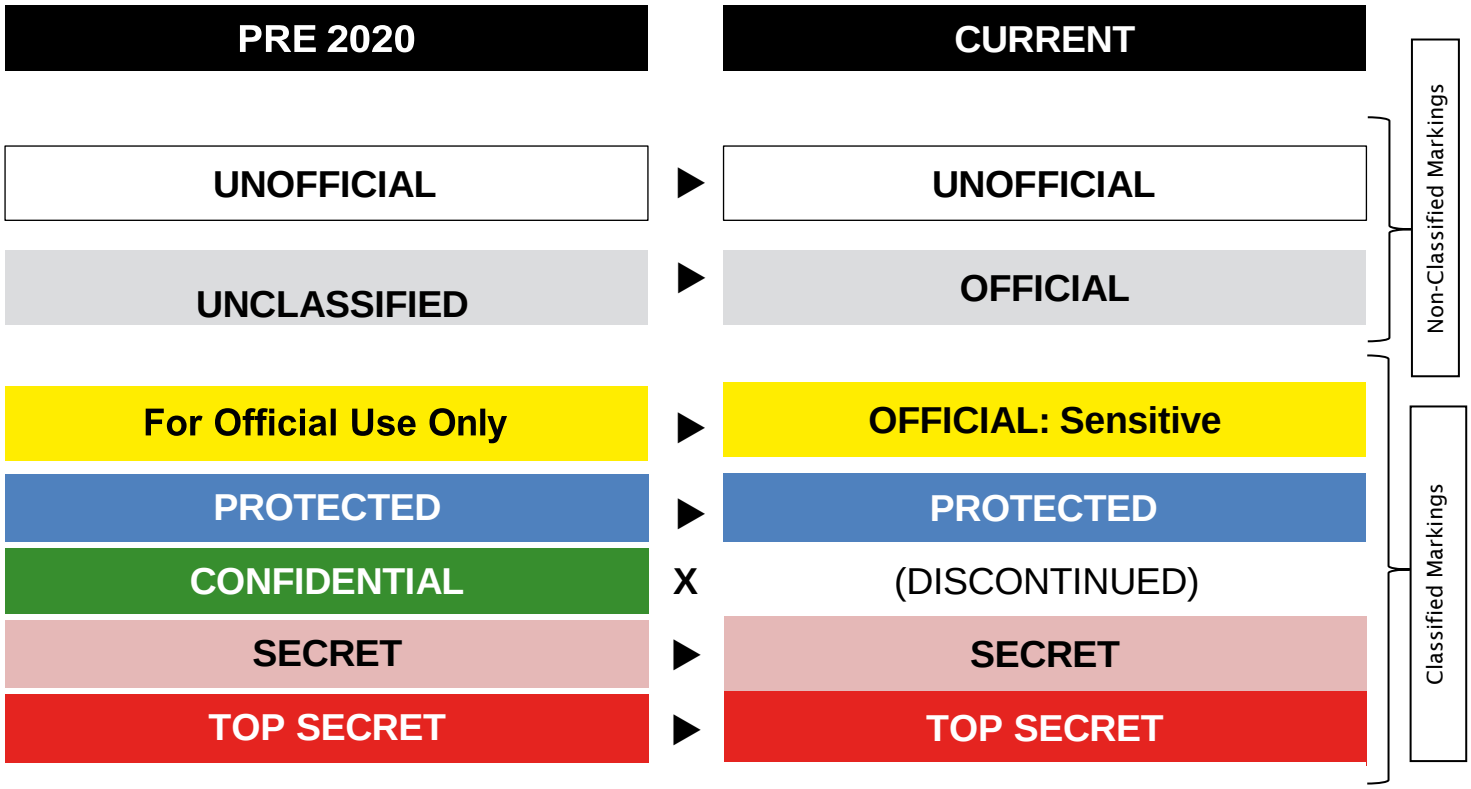
These changes simplify the assessment and protection of Official Information. They also align with the Australian Government *Information Security Manual* (ISM).

The updated classification system now has six* levels:

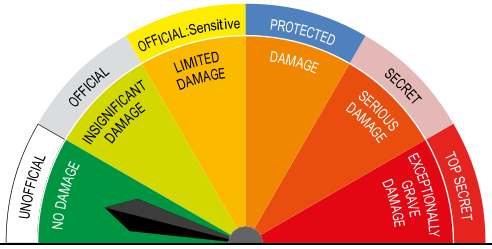
- UNOFFICIAL – no change
- OFFICIAL – replaces UNCLASSIFIED
- OFFICIAL: Sensitive – replaces FOR OFFICIAL USE ONLY (FOUO)
- PROTECTED – no change
- SECRET – no change
- TOP SECRET – no change.

*__Note:__ In August 2023, PSPF Policy 8: Classification System was amended to change the OFFICIAL: Sensitive Dissemination Limiting Marker (DLM) to a security classification. Minimum protections and handling requirements for OFFICIAL: Sensitive remain the same.

Old to New Mapping Guide



UNOFFICIAL



The UNOFFICIAL marker is used to identify information that is not related to your work for Defence.

Even if you are using your Defence email address to send or receive emails, the information may not be OFFICIAL.

Examples of UNOFFICIAL Information include:

- an invitation to a birthday party
- calling your mechanic about a car service
- arranging tennis coaching for the weekend.

Social Media

Our use of social media at home and work is increasing every day. The line between our professional and private lives is blurring.

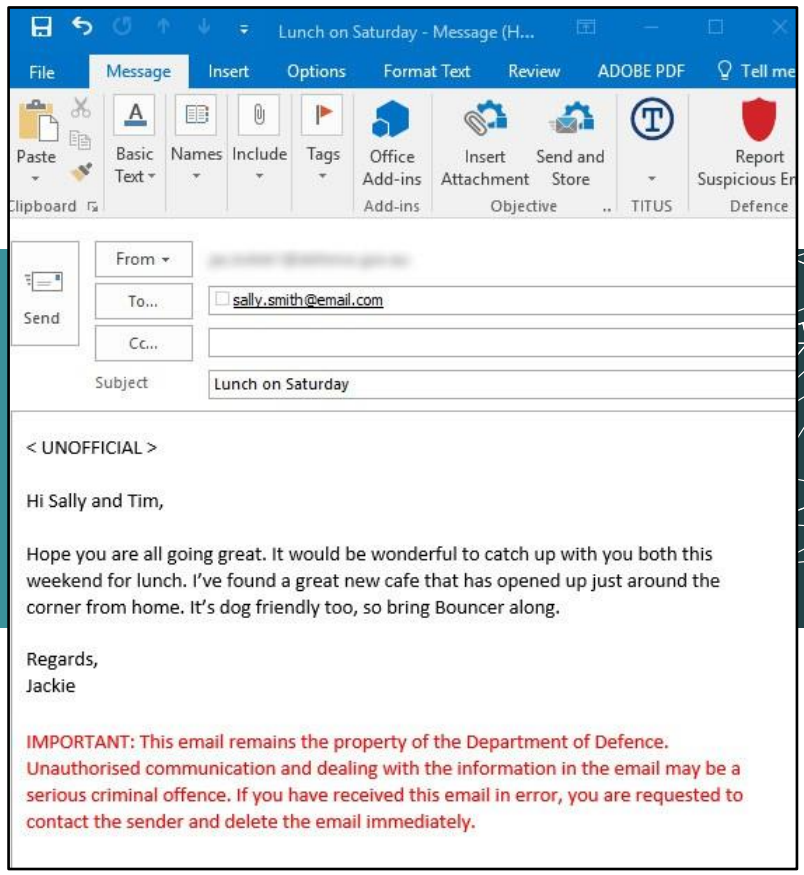
While working with Defence you may use social media personally. Make sure your comments, photos and online associations do not compromise operational or personal security.

Take a moment to reflect before you share any personal information on social media or recruitment platforms. You should consider if the information could cause privacy and security issues for Defence, yourself or your family.

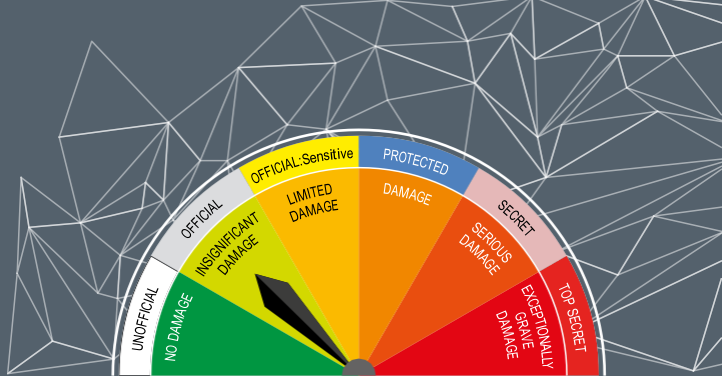
Refer to the *Defence Social Media Policy*, which can be accessed in the Defence Media and Communication Policy.

Business Impact Level: Nil

UNOFFICIAL Information is not part of your work for Defence.



OFFICIAL



All information relating to your work for Defence is Official Information. This information is an official record and it provides evidence of what Defence has done and why.

Official Information includes material held in any format including:

- written documents, reports, memoranda, letters, emails, and notes
- digital information stored on a computer, a video camera or a mobile device
- information which is known to an agency but which has not yet been recorded in writing or otherwise.

The majority of Defence information created for routine business operations and services, is usually marked as OFFICIAL.

Information marked as OFFICIAL may be shared on approved systems with people who have a *Need-to-Know*.

Disclaimer: The following examples of Official Information are for your reference only. You must assess the information each and every time before applying a protective marker.

Examples of Official Information may include:

- hand written notes that you write at a Defence meeting
- an email to a work colleague about a Defence matter
- information prepared for public access or circulation, such as websites or Frequently Asked Questions.

Business Impact Level: Low

If this information was leaked or made public, there would be **insignificant damage** to people, organisations or government. It could cause:

- minor issues for routine business operations and diplomatic activities
- minor impact to Defence assets or budget
- no issues with legislation, commercial confidentiality or legal requirements.

Public release of Official Information

Defence publishes a range of Official Information that is freely accessible to the general public as part of the Commonwealth's Information Publication Scheme including:

- Annual Reports
- White Papers
- Website content
- Speeches
- Media releases.

This information has been through an approval process and is cleared for public review and access. Information assessed as OFFICIAL may only be released publicly in accordance with the Defence Media and Communication Policy.

Access

There are no security clearance requirements for access, however, the *Need-to-Know* principle does apply.

Filing

A file covering is not required.

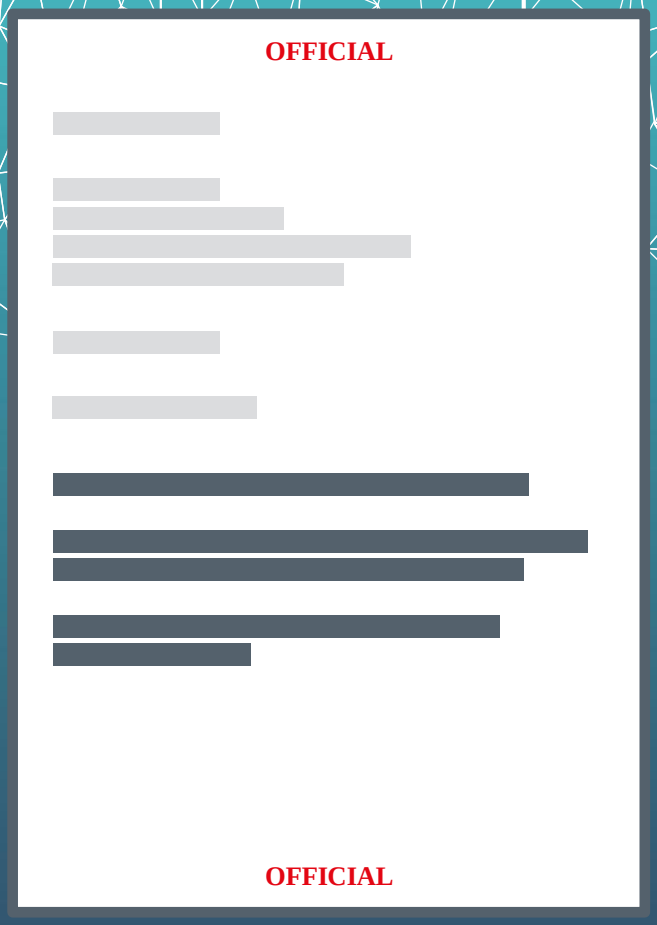
Physical Storage

Storage in a lockable container is recommended in Zone One in accordance with the Archives Act. In Zone Two and above, secured from unauthorised access.

Speak to your Security Officer if you are unsure which security zone you are in.

Registering

A Classified Document Register is not required.



All information relating to your work for Defence is Official Information. The majority of information created by Defence for routine business operations and services is Official Information

Removal

No security requirements.

Copying

You should only make copies if you need to.

Disposal

Ensure compliance with Defence records management policy.

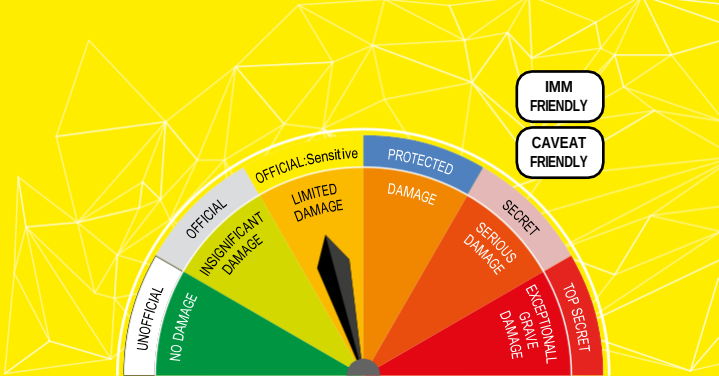
Physical Transfer

It is recommended to use an opaque envelope with the classification clearly identified.

Digital Transfer

It is recommended that information is encrypted if sent over a public network.

OFFICIAL: Sensitive



The OFFICIAL: Sensitive marker is a Classified information marker which identifies Official Information that also contains sensitive material. The sensitivity of the material requires an additional layer of protection to the standard Official Information. Sensitive information is usually information that would affect the reputation or safety of a person, an organisation or Defence.

The OFFICIAL: Sensitive marker protects sensitive information by limiting its access and use to a more specific purpose (e.g. a *Need-to-Know*). OFFICIAL: Sensitive Information can only be shared with people who *Need-to-Know*.

Disclaimer: The following examples of Official Information that may be marked as OFFICIAL: Sensitive, are for your reference only. You must assess the information each and every time before applying a protective marker.

Examples of OFFICIAL: Sensitive Information may include:

- procurement details for a Defence industry project
- standard operating procedures.

In addition to the OFFICIAL: Sensitive marker, you can also apply Information Management Markers (IMMs) to identify information that is subject to non-security related restrictions on access and use. These are: legal privilege, legislative secrecy, and personal privacy.

OFFICIAL: Sensitive information is an attractive target because it is easier to access and a substantial amount of it exists. The capture and assessment of a large amount of OFFICIAL: Sensitive information, could reveal strategic intelligence about Defence personnel and operations.

Business Impact Level: Low to Medium

If this information was leaked or made public, there would be **limited damage** to people, organisations or government. It could cause:

- Defence's business functions to weaken
- $10m to $100m damage to Defence assets
- minor loss of confidence in government
- suffering, harm or injury to someone, but not endanger their life.

Access

There are no security clearance requirements for access, however, the *Need-to-Know* principle does apply.

Filing

A yellow file cover is recommended.

Physical Storage

In Zones One–Five, use a lockable container.

Speak to your Security Officer if you are unsure which security zone you are in.

Registering

A Classified Document Register (CDR) is not required.*

*OFFICIAL: Sensitive material marked with the NATIONAL CABINET caveat must be treated as Accountable Material. Printed material must be registered in a CDR and electronic copies stored on Objective with access limited to those with a Need-to-Know.

OFFICIAL: Sensitive

(O)

(O:S)

(O)

OFFICIAL: Sensitive

The information requiring the highest level of protection determines the overall protection level of the document.

Paragraph two is OFFICIAL: Sensitive – indicated using (O:S) – therefore the overall protection level of the document is OFFICIAL: Sensitive.

Assessing and marking each section or paragraph may be useful, but is not mandatory.

Removal

Only remove documents if you need to. E.g: to take to a meeting.

Keep the information with you at all times and secured from unauthorised access.

Copying

You should only make copies if you need to.

Disposal

Use any Security Construction and Equipment Committee (SCEC) endorsed shredder.

Ensure compliance with Defence records management policy.

Physical Transfer

Protect hard-copy information from unauthorised viewing or access.

Within the building

1. Handed directly to the person.

OR

2. Use an opaque envelope with the classification clearly identified.
   - Then use the Defence internal mail system.

Within Australia

1. Use an opaque envelope that does not give any indication of the classification.

   Then delivered by hand to the person.

OR

2. Use Defence mail system.

OR

3. Use Australia Post or commercial courier.
   - Check whether the original author states you must get a delivery confirmation receipt.

International

Use the double enveloping method.

Use the DFAT courier service.

Ensure you get a delivery confirmation receipt.

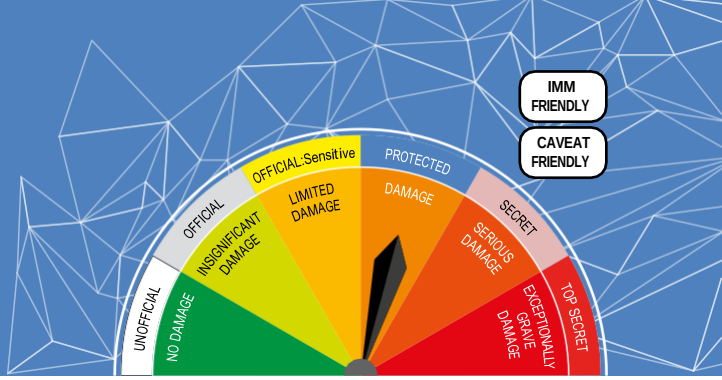
Digital Transfer

Communicate information over Official networks or above.

You must encrypt OFFICIAL: Sensitive information when transmitting it over a public network, or through an unsecured space (including Zone One security areas).

OFFICIAL: Sensitive information can only been sent unencrypted if a risk assessment has been conducted, and the residual security risk is accepted by Defence.

PROTECTED



The PROTECTED information marker is a Classified information marker. It is the second of the four security 'classifications'. The PROTECTED classification is used to identify and protect valuable, important and sensitive information. Compromise of PROTECTED information could cause damage to Defence or Australia.

Disclaimer: The following examples of Official Information that may be marked as PROTECTED, are for your reference only. You must assess the information each and every time before applying a protective marker.

Examples of PROTECTED information include:

- a Cabinet Submission marked PROTECTED CABINET
- threat reports to support risk assessments for key events. E.g. Open Days, Anzac Day processions and movements of VIPs.

PROTECTED information is an attractive target for domestic or international sources, who want to capture large amounts of information and data. Aggregation of this information can reveal considerable details about the capabilities and movements of Defence assets. This could impact Defence's ability to function.

Business Impact Level: High

If this information was leaked or made public, it would damage people, organisations or government.
It could cause:

- disruption to one of Defence's main functions
- $100m to $10b damage to Defence assets or budget
- major loss of confidence in government
- suffering or life threatening injury.

Access

You need a Baseline security clearance and a *Need-to-Know* to access.
PROTECTED information can be accessed via a PROTECTED accredited network, such as the Defence Protected Network (DPN).

Filing

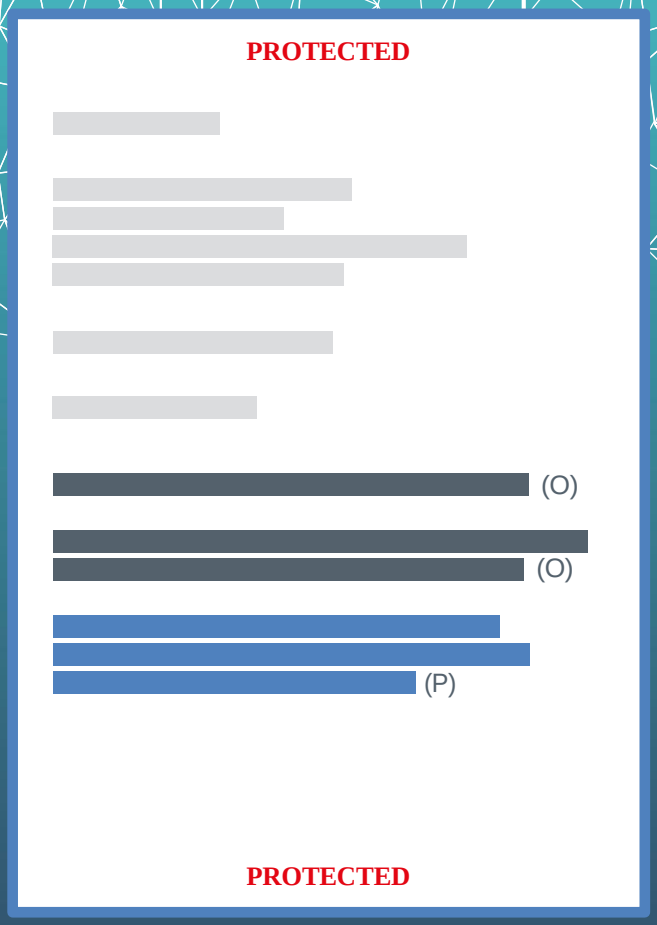
Use a blue PROTECTED file cover.
For more information, ask your Security Officer.

Physical Storage

In Zone One, ongoing storage not recommended. If unavoidable, store in a SCEC Class C container. In Zones Two & Three, store in a SCEC Class C container.
In Zones Four & Five, use a lockable container.
Speak to your Security Officer if you are unsure which security zone you are in.

Registering

Official Information that is classified at the 'PROTECTED' level **AND** is defined as Accountable material must be registered. Printed material must be registered in a Classified Document Register (CDR) and electronic copies stored on Objective. Official Information classified at the 'PROTECTED' level, but not defined as Accountable material, is recommended to be registered in a CDR.



The information requiring the highest level of protection determines the overall protection level of the document.

Paragraph three is PROTECTED – indicated using (P) – therefore the overall protection level of the document is PROTECTED.

Assessing and marking each section or paragraph may be useful, but is not mandatory.

Removal

Only remove documents if you need to. E.g: to take to a meeting.

Keep the information with you at all times and in a SCEC approved briefcase, satchel or pouch.

Copying

You should only make copies if you need to.

Accountable material must not be copied or reproduced by anyone other than the originator. If extra copies of such documents are required, additional copies are to be requested from the originator. Information must not to be extracted from accountable material without the permission of the originator.

Disposal

Use a SCEC Class B shredder or above.

Ensure compliance with Defence records management policy.

Physical Transfer

Protect hard-copy information from unauthorised viewing or access.

Within the building

1. Handed directly to the person.

OR

2. Use an opaque envelope with the classification clearly identified.
   - Then place in a SCEC approved briefcase, satchel or pouch. (Ask your Security Officer).
   - Use an authorised messenger to deliver directly to the person. (Ask your Security Officer).
   - Check whether the original author states you must get a delivery confirmation receipt.

Within Australia

1. Use the double enveloping method.

   Use a SCEC endorsed overnight courier to deliver directly to the person.

OR

2. Use an opaque envelope that does not give any indication of the classification.
   - Then place in a SCEC approved briefcase, satchel or pouch.
   - Use an authorised messenger to deliver directly to the person.
   - Ensure you get a delivery confirmation receipt.

International

Use the double enveloping method.

Use the DFAT courier service.

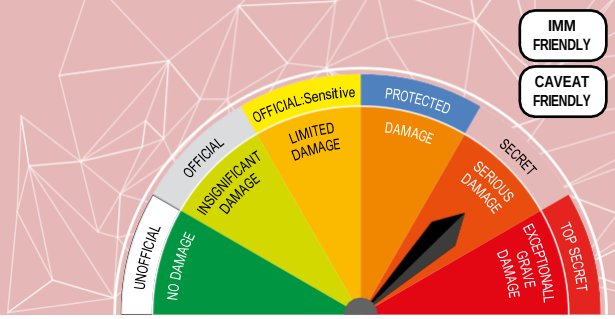
Ensure you get a delivery confirmation receipt.

Digital Transfer

Communicate information over PROTECTED networks or above.

Encrypt PROTECTED information that is not transferred over a PROTECTED network or above.

SECRET



SECRET is the second highest classification and is used to identify and protect very valuable, important and sensitive information. Compromise of SECRET information could cause **serious damage** to Defence or Australia.

Disclaimer: The following examples of Official Information that may be marked as SECRET, are for your reference only. You must assess the information each and every time before applying a protective marker.

Examples of SECRET information may include:

- highly sensitive technology unique and reserved for Australian use only
- tactical warfighting publications
- cryptographic and communications technology.

Access to SECRET information is limited to a much smaller number of personnel. Remember, if you incorrectly over-classify information, a military operation could fail because information could not be accessed in time. Over-classification also increases physical storage requirements and cost.

SECRET information is a very attractive target for our enemies. While the processes for managing this information are not as strict as for TOP SECRET, appropriate measures must be taken and followed for creation, access, use, distribution and storage.

Caveats and Codewords can also be used for SECRET information to further restrict access and distribution. Releasability caveats such as Australian Eyes Only (AUSTEO) or Australian Government Access Only (AGAO) may be applied and the "Charlie" compartment begins at the SECRET classification.

A Classified Document Register (CDR) must be used by Defence Industry partners to record physical versions and copies of SECRET documents.

Protection of our highly sensitive and valuable information means Defence and the Australian government can maintain:

- national security
- sovereign capability
- our reputation with domestic and international agencies.

Business Impact Level: Extreme

If this information was leaked or made public, there would be **serious damage** to people, organisations or government. It could cause:

- the disruption of all Defence functions
- the collapse of political stability in Australia
- prevention of major policies
- financial damage to an Australian industry sector
- suffering and loss of life.

Access

You need Negative Vetting 1 security clearance and a *Need-to-Know* to access.
SECRET information can be accessed via a SECRET accredited network, such as the Defence Secret Network (DSN).

Filing

Use a pink SECRET file cover.
For more information, ask your Security Officer.

Physical Storage

In Zones One & Two, storage not permitted. In Zone Three, store in a SCEC Class B container or above. In Zones Four & Five, store in a SCEC Class C container or above.
Speak to your Security Officer if you are unsure which security zone you are in.

Registering

Official Information classified at the 'SECRET' level, but not defined as Accountable material, is strongly recommended to be registered in a Classified Document Register.

Defence industry partners must use a Classified Document Register for all information classified at SECRET, and record all access, copying and removal. A file census is required at least every two years.

The information requiring the highest level of protection determines the overall protection level of the document.

Paragraph three is SECRET – indicated using (S) – therefore the overall protection level of the document is SECRET.

Assessing and marking each section or paragraph may be useful, but is not mandatory.

Removal

Only remove documents if you need to. E.g: to take to a meeting.

You need authorisation from the person in charge of the information.

Keep the information with you at all times and in a SCEC approved briefcase, satchel or pouch.

Copying

You should only make copies if you need to.

All copies must be numbered (e.g. x of xx).

All copies must be registered, including how many copies were made and who they were given to.

When a document classified 'SECRET' or 'TOP SECRET' is printed from Objective for manual distribution, the document is to include the Object ID.

Any safeguards applied to the original documents also apply to copies.

Disposal

Only use a SCEC Class A cross shredder.

Ensure compliance with Defence records management policy.

Physical Transfer

Protect hard-copy information from unauthorised viewing or access.

Within the building

1. Hand directly to the person.

OR

2. Use an opaque envelope with the classification clearly identified.
   - Then place in a SCEC approved briefcase, satchel or pouch. (Ask your Security Officer).
   - Use an authorised messenger to deliver directly to the person. (Ask your Security Officer).
   - Check whether the original author states you must get a delivery confirmation receipt.

Within Australia

Use the double enveloping method.

Then place in a SCEC approved briefcase, satchel or pouch.

Use an authorised messenger or SCEC endorsed SAFEHAND courier to deliver directly to the person.

Ensure you get a delivery confirmation receipt.

International

Use the double enveloping method.

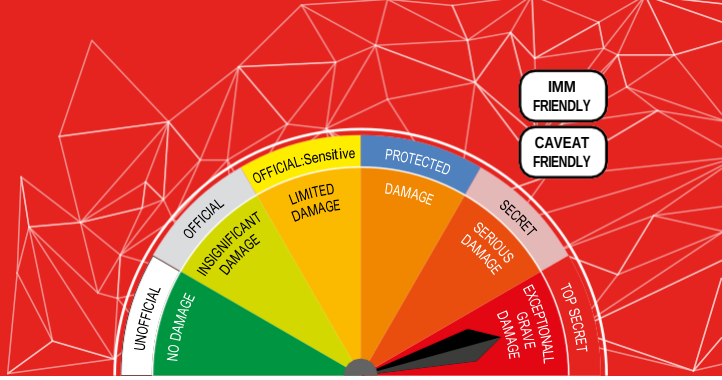
Use the DFAT courier service.

Ensure you get a delivery confirmation receipt.

Digital Transfer

You can communicate SECRET information using the Defence Secret Network (DSN).

TOP SECRET



TOP SECRET is the highest level of classified information used by Defence. It protects our most sensitive and valuable information.

Creation, access, use, replication and storage of TOP SECRET information must be strictly managed. This ensures the information is protected appropriately and prevents its unauthorised release or disclosure.

Disclaimer: The following examples of Official Information that may be marked as TOP SECRET are for your reference only. You must assess the information each and every time before applying a protective marker.

Examples of TOP SECRET information may include:

- intelligence information regarding foreign capabilities or operations
- operational plans
- sensitive capability plans.

Codewords, compartments and caveats may also be added to this classification, to further restrict access and use of the information. Access to Codeword or Compartmented Information requires additional briefings referred to as 'compartment briefs'. Standard compartment briefs include Charlie, Delta and Echo etc. You will only have access to this information if you have been briefed into that compartment.

TOP SECRET information is an extremely attractive target. Any compromise could cause "exceptionally grave damage" to national security. If you are responsible for unauthorised release of Top Secret information, you could face criminal charges.

By protecting our most sensitive and valuable information, Defence and the Australian Government can maintain:

- national security
- sovereign capability
- our reputation with domestic and international agencies.

Business Impact Level: Catastrophic

If this information was leaked or made public, there would be **exceptionally grave damage** to people, organisations or government. It could cause:

- the collapse of stability in Australia or 'friendly' or 'allied' countries
- the collapse of the Australian economy
- international conflict
- the collapse of all major national infrastructure
- widespread suffering or loss of life.

Access

You need Negative Vetting 2 and a *Need-to-Know* to access.
Some compartmented information requires Positive Vetting to access.
TOP SECRET information can be accessed via a TOP SECRET accredited network.

Filing

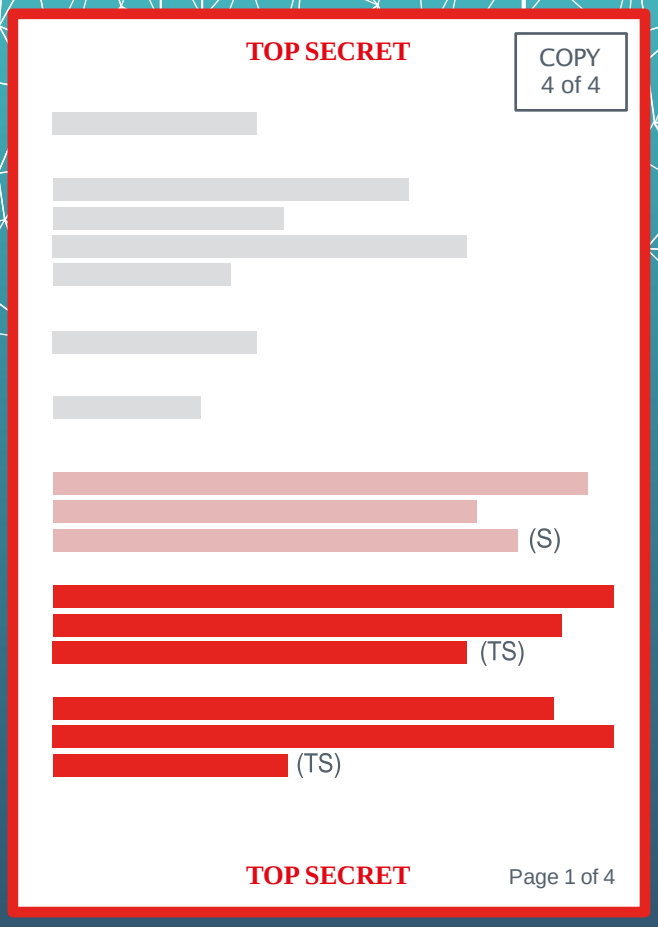
Use a red TOP SECRET file cover.
For more information, ask your Security Officer.

Physical Storage

Zones One & Two, storage not permitted.
Zone Three, storage not normally permitted (In exceptional circumstances SCEC Class A for a maximum of five days).
Zone Four, storage not normally permitted (In exceptional circumstances SCEC Class B).
Zone Five, store in a SCEC Class B or above.
Speak to your Security Officer if you are unsure which security zone you are in.

Registering

Use a separate Classified Document Register and record all access, copying and removal.
Complete a file census at least every two years.



The information requiring the highest level of protection determines the overall protection level of the document.

Paragraphs two and three are TOP SECRET – indicated using (TS) – therefore the overall protection level of the document is TOP SECRET.

Assessing and marking each section or paragraph may be useful, but is not mandatory.

Removal

Only remove documents if you need to. E.g.: to take to a meeting.

You need authorisation from the person in charge of the information.

Keep the information with you at all times and in a SCEC approved briefcase, satchel or pouch.

Seek advice from ASIO if you must take the documents to a meeting or conference.

Consider if it's better to send the documents ahead by SAFEHAND.

Disposal

You should destroy the information as soon as no one needs it anymore. Ensure compliance with Defence records management policy.

Only use a SCEC Class A cross shredder.

Two people need to be there when the document is being destroyed. They both need to sign a destruction certificate.

Copying

You should only make copies if you need to.

All copies must be numbered (e.g. x of xx).

All copies must be registered, including how many copies were made and who they were given to.

When a document classified 'SECRET' or 'TOP SECRET' is printed from Objective for manual distribution, the document is to include the Object ID.

Any safeguards applied to the original documents also apply to copies.

Physical Transfer

Protect hard-copy information from unauthorised viewing or access.

Within the building

1. Hand directly to the person.

OR

2. Use an opaque envelope with the classification clearly identified.
   - Then place in a SCEC approved briefcase, satchel or pouch. (Ask your Security Officer).
   - Use an authorised messenger to deliver directly to the person. (Ask your Security Officer).
   - Ensure you get a delivery confirmation receipt.

Within Australia

Use the double enveloping method.

Then place in a SCEC approved briefcase, satchel or pouch.

Use an authorised messenger or SCEC endorsed SAFEHAND courier to deliver directly to the person.

Ensure you get a delivery confirmation receipt.

International

Use the double enveloping method.

Use the DFAT courier service.

Ensure you get a delivery confirmation receipt.

Digital Transfer

You can communicate TOP SECRET information over a TOP SECRET accredited network.

Information Management Markers

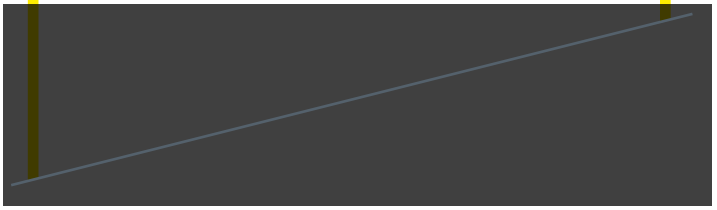
An Information Management Marker (IMM) is an optional marker that indicates that there are legislative protections for distribution of the information.

IMMs are not classifications and must appear with an appropriate protective marker or classification.

Use an IMM to further restrict information to people with a *Need-to-Know*. Defence uses the following three:

- **Legal privilege** – to restrict access and use of information exchange between a lawyer and client for legal advice and proceedings.
- **Legislative secrecy** – to restrict access and use of information where rules for its release are specified in Commonwealth legislation.
- **Personal privacy** – to restrict access and use of personal information that is collected for business purposes as specified under the *Privacy Act 1988* (Cth).

OFFICIAL: Sensitive
Legislative secrecy



OFFICIAL: Sensitive
Legal privilege

Legal privilege
OFFICIAL: Sensitive

OFFICIAL: Sensitive
Personal privacy

Personal privacy
OFFICIAL: Sensitive

Caveats

A caveat identifies that the information needs special protections in addition to those indicated by the protective marking.

Caveats are not classifications and must appear with an appropriate protective marking.

Caveats can only be applied to information classified as PROTECTED or above.

The originator must approve any changes to, or removal of a caveat.

A caveat may be used to provide additional, special protections where the protective marking is not sufficient. There are four categories of caveats:

- Special handling instructions (including CABINET)
- Releasability caveats (AGAO, AUSTEO)
- Sensitive compartments (Codewords)
- Foreign government markers.

Special Handling Instructions

Use special handling instructions to indicate particular precautions for information handling.

CABINET – identifies any material that:

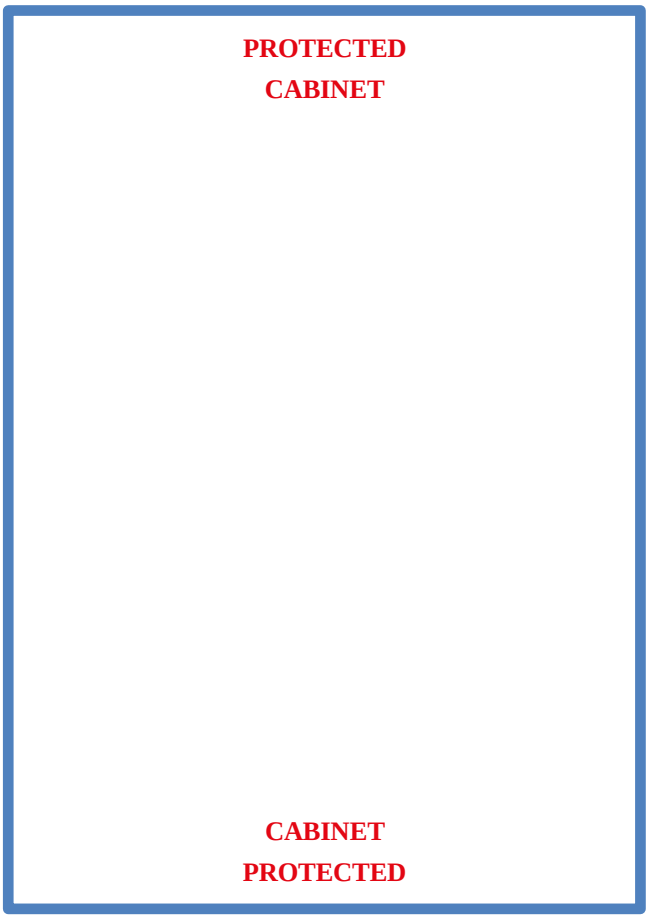
- is prepared for the purpose of informing the Cabinet
- reveals the decisions and/or deliberations of the Cabinet
- is prepared by departments to brief their minister's on proposals for Cabinet consideration
- has been created for the purpose of informing a proposal to be considered by the Cabinet.

This caveat must only be applied to information marked PROTECTED and above and has a strict *Need-to-Know*.

Note: CABINET is accountable material and must be registered, handled and stored in accordance with the DSPF.

EXCLUSIVE FOR (*name of a person*) – identifies material for access by a named recipient, position title or designation only.

- This caveat can be applied to material protectively marked PROTECTED and above.



Releasability caveats

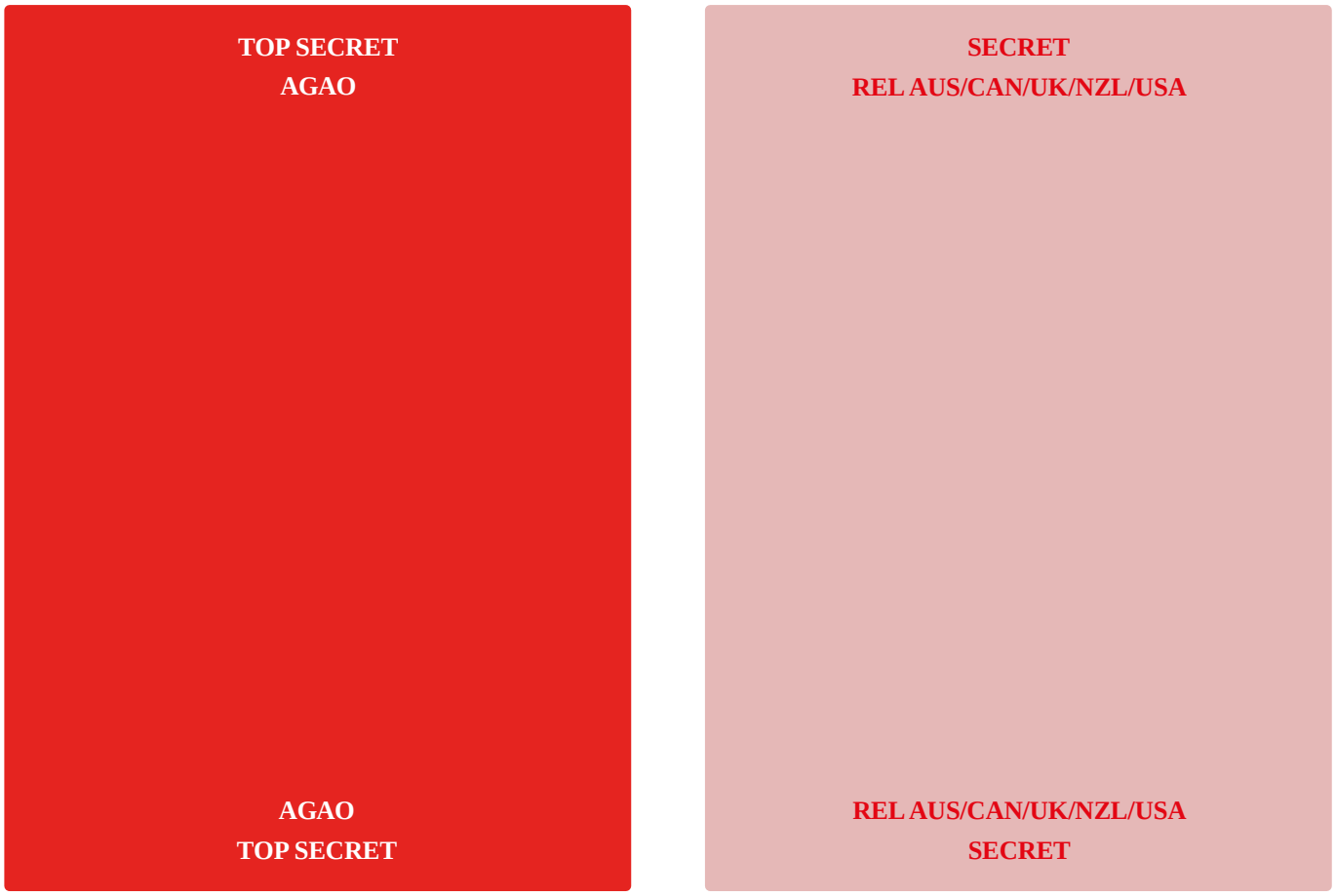
Use Releasability caveats to limit access to information. They can be applied to PROTECTED information and above, but must only be on a Defence network accredited SECRET or above (e.g. the DSN).

- **Australian Eyes Only (AUSTEO)** –Access is strictly Australian citizens only. Holding of additional citizenship does not preclude access.
- **Australian Government Access Only (AGAO)** – indicates that appropriately-cleared Australian citizens, and appropriately-cleared representatives of Five-Eyes foreign governments on exchange or long-term posting or attachment in the National Intelligence Community and the Department of Defence can access the information.

Agencies other than members of the National Intelligence Community (ONI, ASD, AGO, ASIO, ASIS, ACIC, AFP, AUSTRAC, DIO and Home Affairs), and Defence and the Australian Submarine Agency must treat AGAO material as if it were marked AUSTEO.

- **Releasable to** – identifies information which has been, or is releasable to the indicated foreign countries.

Note: When developing a document that will carry a Releasability caveat (AUSTEO, AGAO or Releasable to), it must be developed and saved using the DSN.


TOP SECRET
AGAO
AGAO
TOP SECRET
SECRET
REL AUS/CAN/UK/NZL/USA
REL AUS/CAN/UK/NZL/USA
SECRET

Foreign Government Markers

Foreign government marker caveats are applied to material created by Australian agencies from foreign information sources.

There may be further safeguarding requirements dictated by Security of Information Agreements & Arrangements.

Foreign government marker caveats require protection that is at least equivalent to the protection required by the foreign government providing the source material.

SECRET
UK/NZL

UK/NZL
SECRET

Country codes can be obtained through *International Standard ISO3166-1:2013*.

Codewords

Each Codeword identifies a special *Need-to-Know* 'compartment'. A compartment is a mechanism for restricting information access to defined individuals.

These individuals have been 'briefed' on the particular sensitivities of that information compartment and any special rules that may apply.

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

A briefing is required before access can be provided to caveated material that involves a Codeword. Access to Codeword material may also need a certain level of security clearance, as well as other additional requirements.

TOP SECRET
CODEWORD1234

CODEWORD1234
TOP SECRET

Information Handling Summaries

Sensitive and security classified information or resources should only be shared with people who *Need-to-Know*.

Ongoing Access to Information

Clearance Levels	Official Information					
	OFFICIAL	OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET	Sensitive Compartmented Information E.g. Codewords
No Clearance	✓*	✓*				
Baseline	✓	✓	✓			
Negative Vetting Level 1 (NV1)	✓	✓	✓	✓		✓
Negative Vetting Level 2 (NV2)	✓	✓	✓	✓	✓	✓
Positive Vetting (PV)	✓	✓	✓	✓	✓	✓

* There are no security clearance requirements for access, however, a *Need-to-Know* applies.

Transporting Information

Protective Marking/Classification	Minimum Protection	
	Within Australia	International
OFFICIAL OFFICIAL: Sensitive (including any IMM)	• Sealed single envelope	• Sealed single envelope
PROTECTED	• Double enveloping • Receipt required • SCEC-endorsed courier	• Double enveloping • Receipt required • DFAT courier or authorised officer
SECRET	• Double enveloping • SCEC-endorsed pouch or security briefcase • Receipt required • Delivered direct by authorised messenger or SCEC-endorsed courier	• Double enveloping • Receipt required • DFAT courier or authorised officer
TOP SECRET	• Double enveloping • SCEC-endorsed pouch or security briefcase. • Receipt required • Delivered direct by authorised messenger or safe hand courier	• Double enveloping • Receipt required • DFAT courier or authorised officer

Information and Asset Storage

Protective Marking/Classification	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
OFFICIAL	Lockable container	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access
OFFICIAL: Sensitive	Lockable container	Lockable container	Lockable container	Lockable container	Lockable container
PROTECTED	Ongoing storage not recommended, if unavoidable SCEC Class C	SCEC Class C	SCEC Class C	Lockable container	Lockable container
SECRET	Not permitted	Not permitted	SCEC Class B	SCEC Class C	SCEC Class C
TOP SECRET	Not permitted	Not permitted	Not normally permitted. (In exceptional circumstances SCEC Class A)	Not normally permitted. (In exceptional circumstances SCEC Class B)	SCEC Class B
CONFIDENTIAL (historical handling protections remain)	Not permitted	SCEC Class B	SCEC Class C	SCEC Class C	Determined by a security risk assessment

Destroying Classified Information

Protective Marking/Classification	Destruction Method
OFFICIAL	• Shredder
OFFICIAL: Sensitive (including any IMM, but not including with caveat/special handling requirements i.e. accountable material.)	
PROTECTED	• Class B shredder
SECRET	• Class A cross shredder
TOP SECRET	• Class A cross shredder • Two person supervise and certify • Destroy information as soon as possible

The destruction of all Accountable material requires two people to supervise and certify the destruction regardless of its protective marking or classification.

Accountable material

Accountable material may include:

- TOP SECRET information
- all Codeword information
- select special handling instructions
- CABINET material
- any classified information deemed Accountable material by the originator.

Acronyms

AGAO	Australian Government Access Only
AUSTEO	Australian Eyes Only
ASA	Australian Submarine Agency
ASIO	Australian Security Intelligence Organisation
BIL	Business Impact Level
CDR	Classified Document Register
DFAT	Department of Foreign Affairs and Trade
DPN	Defence Protected Network
DSN	Defence Secret Network
DSPF	Defence Security Principles Framework
ICT	Information Communication Technology
IMM	Information Management Marker
ISM	Information Security Manual
NV1	Negative Vetting Level 1
NV2	Negative Vetting Level 2
PSPF	Protective Security Policy Framework
PV	Positive Vetting
SCEC	Security Construction and Equipment Committee
SCIF	Sensitive Compartmented Information Facility
VIP	Very Important Person

Assessing and Protecting Official Information Course

The aim of the course is to provide those who handle Official Information with the knowledge and skills necessary to perform their duties and fulfil their requirements under the Defence Security Principles Framework (DSPF).

The course is available to Defence staff in eLearning format via LXP.

Further Information

Security information can be found via:

- Your Security Officer
- Search for 'Assessing and protecting official information' at www.defence.gov.au
- **1800DEFENCE** (1800 333 362).